M.F.

EO/US
PCT/DK99/00331

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing: 13 January 2000 (13.01.00)	
International application No.: PCT/DK99/00331	Applicant's or agent's file reference: 21487 PC1
International filing date: 16 June 1999 (16.06.99)	Priority date: 03 July 1998 (03.07.98)
Applicant: GLÜCKSTAD, Jesper	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

26 November 1999 (26.11.99)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer: J. Zahra Telephone No.: (41-22) 338.83.38

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04K1/00 G02B27/52 G02B27/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04K G02B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JAVIDI: PHYSICS TODAY, vol. 50, no. 3, March 1997 (1997-03), pages 27-32, XP002116193 AMERICAN INSTITUTE OF PHYSICS, NEW YORK., US ISSN: 0031-9228 cited in the application page 30 -page 31; figure 4 ---	1,4,14, 28,31, 41,42,47
A	PATENT ABSTRACTS OF JAPAN vol. 016, no. 281 (P-1375), 23 June 1992 (1992-06-23) & JP 04 073790 A (NIPPON TELEGR & TELEPH CORP), 9 March 1992 (1992-03-09) abstract ---	1,11,28, 37

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 September 1999	06/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	von Moers, F

2

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 148 316 A (HORNER JOSEPH L ET AL) 15 September 1992 (1992-09-15) column 2, line 41 - line 69; figure 1	1,11,28, 37
A	WO 96 34307 A (RISOE FORSKNINGSCENTER ;GLUECKSTAD JESPER (DK)) 31 October 1996 (1996-10-31) cited in the application page 9; figure 1	1,3,28, 30

2

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
JP 04073790	A	09-03-1992	NONE			
US 5148316	A	15-09-1992	NONE			
WO 9634307	A	31-10-1996	AU	5496396	A	18-11-1996
			EP	0830632	A	25-03-1998
			JP	11504129	T	06-04-1999

PATENT COOPERATION TREATY

REC'D 12 OCT 2000
WIPO PCT

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 21487 PC1	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/DK99/00331	International filing date *(day/month/year)* 16/06/1999	Priority date *(day/month/year)* 03/07/1998
International Patent Classification (IPC) or national classification and IPC H04K1/00		
Applicant FORSKNINGSCENTER RISO et,al		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand 26/11/1999	Date of completion of this report 10.10.2000
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Forster, G Telephone No. +49 89 2399 8986

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-31 as originally filed

Claims, No.:

1-49 as originally filed

Drawings, sheets:

1/9-9/9 as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-49
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-49
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-49
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

to section V.

1. The present invention relates to a method and a system for decrypting an encrypted image having a non-encrypted image intensity pattern, according to the features of the independent claims 1 and 28 respectively and to a method of encrypting an image, according to the features of the independent claim 14.

   The closest prior art document appears to be represented by the document 'Securing Information with Optical Technologies', by Javidi, B., PHYSICS TODAY, vol. 50, no. 3, March 1997 (1997-03), pages 27-32, AMERICAN INSTITUTE OF PHYSICS, NEW YORK, US (first document cited in the international search report) and is acknowledged in the opening part of the description.

2. According to the features of the independent claims the inventive step consists in that doubly encrypted optical information is decrypted by radiating light through the encrypted mask, modulating the light with a complex spatial light modulator comprising modulator resolution elements, each modulator resolution element modulating the phase and the amplitude of the electromagnetic radiation, and imaging this light to the output image plane.

   The underlying concept is not disclosed in or rendered obvious by the cited prior art documents. The subject-matter of the independent claims thus fulfils the requirements of Article 33 PCT.

3. The dependent claims contain further details on the subject-matter of the respective independent claims. These dependent claims merely limit the scope of protection sought by the independent claims and are therefore also considered to fulfil the requirements of Article 33 PCT.

to section VII.

1. Reference signs in parentheses have not been inserted in the claims to increase their intelligibility, Rule 6.2(b) PCT.

2. The phrase 'incorporated herein by reference' on page 1, lines 14 and 15 should have been deleted since its precise significance and implications are not clear, Article 5 and 6 PCT.

3. Dependent claim 49 should read 'A system according to ...' and not 'A method according to ...' since this claim is related to a system.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 21487 PCI	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/DK 99/00331	International filing date *(day/month/year)* 16/06/1999	(Earliest) Priority Date *(day/month/year)* 03/07/1998
Applicant FORSKNINGSCENTER RISO et,al		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.
   [ ] filed together with the international application in computer readable form.
   [ ] furnished subsequently to this Authority in written form.
   [ ] furnished subsequently to this Authority in computer readble form.
   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).
3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant.
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [ ] the text is approved as submitted by the applicant.
   [X] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 9

   [X] as suggested by the applicant.
   [ ] because the applicant failed to suggest a figure.
   [ ] because this figure better characterizes the invention.
   [ ] None of the figures.

INTERNATIONAL SEARCH REPORT

International application No
PCT/DK 99/00331

Box III TEXT OF THE ABSTRACT (Continuation of item 5 of the first sheet)

The invention relates to securing of information utilising optical imaging technologies and more specifically to phase encryption and decryption of images. An image is encrypted into a mask having a plurality of mask resolution elements (X_m, Y_m) by encoding the image using eg. a phase mask with an encoded phase value $\phi(X_m, Y_m)$ and an encoded amplitude value a (X_m, Y_m), and by further encrypting the mask (using eg. a spatial light modulator) by addition of an encrypting phase value ϕ_c (X_m, Y_m) to the encoded phase value ϕ (X_m, Y_m) and by multiplication of an encrypting amplitude value a_c (X_m, Y_m) with the encoded phase value a (X_m, Y_m). The method of decrypting comprises the steps of decrypting the mask by radiating electromagnetic radiation towards the mask and inserting into the path of the electromagnetic radiation a complex spatial electromagnetic radiation modulator comprising modulator resolution elements, the decrypting phase value ϕ_d (X_d, Y_d) and the decrypting amplitude value a_d (X_d, Y_d) respectively, of a modulator resolution element (X_d, Y_d) being substantially equal to $-\phi_c$ (X_m, Y_m) and a_c^{-1} (X_m, Y_m).

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DK 99/00331

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04K1/00 G02B27/52 G02B27/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04K G02B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JAVIDI: PHYSICS TODAY, vol. 50, no. 3, March 1997 (1997-03), pages 27-32, XP002116193 AMERICAN INSTITUTE OF PHYSICS, NEW YORK., US ISSN: 0031-9228 cited in the application page 30 -page 31; figure 4 ---	1,4,14, 28,31, 41,42,47
A	PATENT ABSTRACTS OF JAPAN vol. 016, no. 281 (P-1375), 23 June 1992 (1992-06-23) & JP 04 073790 A (NIPPON TELEGR & TELEPH CORP), 9 March 1992 (1992-03-09) abstract ---	1,11,28, 37
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 September 1999	06/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	von Moers, F

2

International Application No
PCT/DK 99/00331

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 148 316 A (HORNER JOSEPH L ET AL) 15 September 1992 (1992-09-15) column 2, line 41 - line 69; figure 1 ---	1,11,28, 37
A	WO 96 34307 A (RISOE FORSKNINGSCENTER ;GLUECKSTAD JESPER (DK)) 31 October 1996 (1996-10-31) cited in the application page 9; figure 1 -----	1,3,28, 30

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DK 99/00331

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 04073790 A	09-03-1992	NONE	
US 5148316 A	15-09-1992	NONE	
WO 9634307 A	31-10-1996	AU 5496396 A	18-11-1996
		EP 0830632 A	25-03-1998
		JP 11504129 T	06-04-1999

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

International Application No.

International Filing Date

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference (if desired) (12 characters maximum) 21487 PC1

Box No. I TITLE OF INVENTION

An Optical Encryption and Decryption Method and System

Box No. II APPLICANT

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

FORSKNINGSCENTER RISØ
Frederiksborgvej 399
P.O.Box 49
DK-4000 Roskilde

☐ This person is also inventor.

Telephone No.

Facsimile No.

Teleprinter No.

State *(that is, country)* of nationality: DK

State *(that is, country)* of residence: DK

This person is applicant for the purposes of: ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

GLÜCKSTAD, Jesper
Voldumvej 45, st.tv
DK-2610 Rødovre

This person is:
☐ applicant only
☒ applicant and inventor
☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: DK

State *(that is, country)* of residence: DK

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

PLOUGMANN, VINGTOFT & PARTNERS A/S
Sankt Annae Plads 11
P.O.Box 3007
DK-1021 Copenhagen K

Telephone No. +45 33 63 93 00

Facsimile No. +45 33 63 96 00

Teleprinter No.

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Box No.V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) *(mark the applicable check-boxes; at least one must be marked)*:

Regional Patent

- ☒ **AP** **ARIPO Patent:** GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, SD Sudan, SZ Swaziland, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT
- ☒ **EA** **Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- ☒ **EP** **European Patent:** AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- ☒ **OA** **OAPI Patent:** BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* ....

National Patent *(if other kind of protection or treatment desired, specify on dotted line)*:

☒	AL	Albania	☒	LS	Lesotho
☒	AM	Armenia	☒	LT	Lithuania
☒	AT	Austria and utility model	☒	LU	Luxembourg
☒	AU	Australia	☒	LV	Latvia
☒	AZ	Azerbaijan	☒	MD	Republic of Moldova
☒	BA	Bosnia and Herzegovina	☒	MG	Madagascar
☒	BB	Barbados	☒	MK	The former Yugoslav Republic of Macedonia
☒	BG	Bulgaria			
☒	BR	Brazil	☒	MN	Mongolia
☒	BY	Belarus	☒	MW	Malawi
☒	CA	Canada	☒	MX	Mexico
☒	CH and LI	Switzerland and Liechtenstein	☒	NO	Norway
☒	CN	China	☒	NZ	New Zealand
☒	CU	Cuba	☒	PL	Poland
☒	CZ	Czech Republic and utility model	☒	PT	Portugal
☒	DE	Germany and utility model	☒	RO	Romania
☒	DK	Denmark and utility model	☒	RU	Russian Federation
☒	EE	Estonia and utility model	☒	SD	Sudan
☒	ES	Spain	☒	SE	Sweden
☒	FI	Finland and utility model	☒	SG	Singapore
☒	GB	United Kingdom	☒	SI	Slovenia
☒	GD	Grenada	☒	SK	Slovakia and utility model
☒	GE	Georgia	☒	SL	Sierra Leone
☒	GH	Ghana	☒	TJ	Tajikistan
☒	GM	Gambia	☒	TM	Turkmenistan
☒	HR	Croatia	☒	TR	Turkey
☒	HU	Hungary	☒	TT	Trinidad and Tobago
☒	ID	Indonesia	☒	UA	Ukraine
☒	IL	Israel	☒	UG	Uganda
☒	IN	India	☒	US	United States of America
☒	IS	Iceland			
☒	JP	Japan	☒	UZ	Uzbekistan
☒	KE	Kenya	☒	VN	Viet Nam
☒	KG	Kyrgyzstan	☒	YU	Yugoslavia
☒	KP	Democratic People's Republic of Korea	☒	ZW	Zimbabwe
☒	KR	Republic of Korea			
☒	KZ	Kazakhstan			
☒	LC	Saint Lucia			
☒	LK	Sri Lanka			
☒	LR	Liberia			

Check-boxes reserved for designating States (for the purposes of a national patent) which have become party to the PCT after issuance of this sheet:

- ☒ AE United Arab Emirates
- ☒ ZA South Africa
- ☐ ....

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation of a designation consists of the filing of a notice specifying that designation and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.)*

Box No. VI PRIORITY CLAIM ☐ Further priority claims are indicated in the Supplemental Box.

Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application: country	regional application:* regional Office	international application: receiving Office
item (1) Denmark	03.07.1998 (3 July 1998)	PA 199800869		
item (2)	15.03.1999 (15 March 99)	PA 199900364		
item (3)				

☒ The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office)* identified above as item(s): (1) + (2)

* *Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used)*:

ISA /EPO

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority)*:

Date *(day/month/year)* Number Country *(or regional Office)*

Box No. VIII CHECK LIST; LANGUAGE OF FILING

This international application contains the following **number of sheets**:

request	:	3
description (excluding sequence listing part)	:	31
claims	:	11
abstract	:	1
drawings	:	9
sequence listing part of description	:	
Total number of sheets	:	55

This international application is **accompanied** by the item(s) marked below:

1. ☒ fee calculation sheet
2. ☒ separate signed power of attorney
3. ☐ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☐ priority document(s) identified in Box No. VI as item(s):
6. ☐ translation of international application into (language):
7. ☐ separate indications concerning deposited microorganism or other biological material
8. ☐ nucleotide and/or amino acid sequence listing in computer readable form
9. ☐ other *(specify)*:

Figure of the drawings which should accompany the abstract: Fig. 9

Language of filing of the international application: English

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Copenhagen, 16 June 1999
Plougmann, Vingtoft & Partners A/S

GHJ

Gert Høy Jakobsen

For receiving Office use only

1. Date of actual receipt of the purported international application:
2. Drawings: ☐ received: ☐ not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:
4. Date of timely receipt of the required corrections under PCT Article 11(2):
5. International Searching Authority (if two or more are competent): ISA /
6. ☐ Transmittal of search copy delayed until search fee is paid.

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 21487 PC1	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/DK99/00331	International filing date *(day/month/year)* 16/06/1999	Priority date *(day/month/year)* 03/07/1998
International Patent Classification (IPC) or national classification and IPC H04K1/00		
Applicant FORSKNINGSCENTER RISO et,al		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand 26/11/1999	Date of completion of this report 10.10.2000
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Forster, G Telephone No. +49 89 2399 8986

Form PCT/IPEA/409 (cover sheet) (January 1994)

I. **Basis of the report**

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-31 as originally filed

Claims, No.:

1-49 as originally filed

Drawings, sheets:

1/9-9/9 as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-49
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-49
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-49
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

to section V.

1. The present invention relates to a method and a system for decrypting an encrypted image having a non-encrypted image intensity pattern, according to the features of the independent claims 1 and 28 respectively and to a method of encrypting an image, according to the features of the independent claim 14.

   The closest prior art document appears to be represented by the document 'Securing Information with Optical Technologies', by Javidi, B., PHYSICS TODAY, vol. 50, no. 3, March 1997 (1997-03), pages 27-32, AMERICAN INSTITUTE OF PHYSICS, NEW YORK, US (first document cited in the international search report) and is acknowledged in the opening part of the description.

2. According to the features of the independent claims the inventive step consists in that doubly encrypted optical information is decrypted by radiating light through the encrypted mask, modulating the light with a complex spatial light modulator comprising modulator resolution elements, each modulator resolution element modulating the phase and the amplitude of the electromagnetic radiation, and imaging this light to the output image plane.

   The underlying concept is not disclosed in or rendered obvious by the cited prior art documents. The subject-matter of the independent claims thus fulfils the requirements of Article 33 PCT.

3. The dependent claims contain further details on the subject-matter of the respective independent claims. These dependent claims merely limit the scope of protection sought by the independent claims and are therefore also considered to fulfil the requirements of Article 33 PCT.

to section VII.

1. Reference signs in parentheses have not been inserted in the claims to increase their intelligibility, Rule 6.2(b) PCT.

2. The phrase 'incorporated herein by reference' on page 1, lines 14 and 15 should have been deleted since its precise significance and implications are not clear, Article 5 and 6 PCT.

3. Dependent claim 49 should read 'A system according to ...' and not 'A method according to ...' since this claim is related to a system.

+ "claims 48'
→ "claim 48" is
same!

A·D

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04K 1/00, G02B 27/52, 27/46	A1	(11) International Publication Number: WO 00/02339 (43) International Publication Date: 13 January 2000 (13.01.00)

(21) International Application Number: PCT/DK99/00331

(22) International Filing Date: 16 June 1999 (16.06.99)

(30) Priority Data:
PA 1998 00869 3 July 1998 (03.07.98) DK
PA 1999 00364 15 March 1999 (15.03.99) DK

(71) Applicant *(for all designated States except US)*: FORSKNINGSCENTER RISØ [DK/DK]; Frederiksborgvej 399, P.O. Box 49, DK-4000 Roskilde (DK).

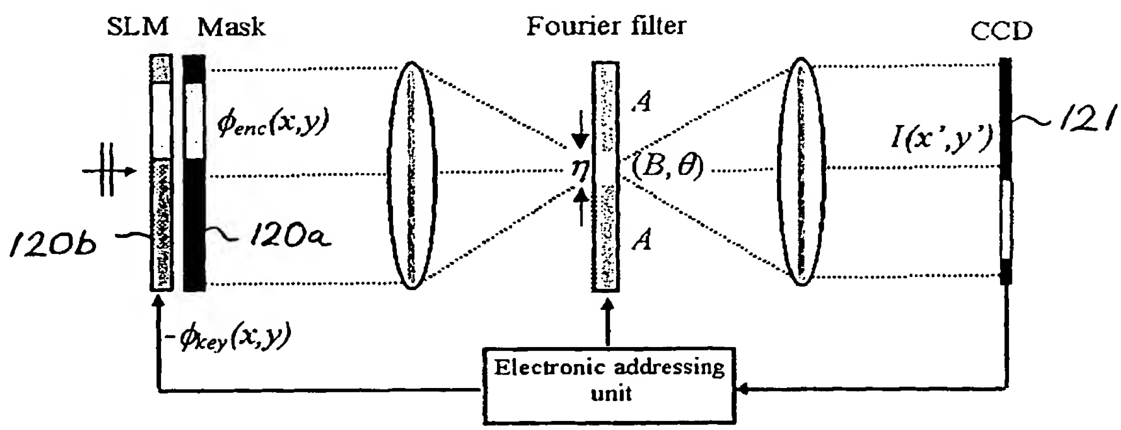
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: GLÜCKSTAD, Jesper [DK/DK]; Voldumvej 45, st. tv, DK-2610 Rødovre (DK).

(74) Agent: PLOUGMANN, VINGTOFT & PARTNERS A/S; Sankt Annae Plads 11, P.O. Box 3007, DK-1021 Copenhagen K (DK).

(81) Designated States: AE, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: AN OPTICAL ENCRYPTION AND DECRYPTION METHOD AND SYSTEM



(57) Abstract

The invention relates to securing of information utilising optical imaging technologies and more specifically to phase encryption and decryption of images. An image is encrypted into a mask having a plurality of mask resolution elements (X_m, Y_m) by encoding the image using e.g. a phase mask with an encoded phase value ϕ (X_m, Y_m) and an encoded amplitude value a (X_m, Y_m), and by further encrypting the mask (using e.g. a spatial light modulator) by addition of an encrypting phase value ϕ_c (X_m, Y_m) to the encoded phase value ϕ (X_m, Y_m) and by multiplication of an encrypting amplitude value a_c (X_m, Y_m) with the encoded phase value a (X_m, Y_m). The method of decrypting comprises the steps of decrypting the mask by radiating electromagnetic radiation towards the mask and inserting into the path of the electromagnetic radiation a complex spatial electromagnetic radiation modulator comprising modulator resolution elements, the decrypting phase value ϕ_d (X_d, Y_d) and the decrypting amplitude value a_d (X_d, Y_d) respectively, of a modulator resolution element (X_d, Y_d) being substantially equal to $-\phi_c$ (X_m, Y_m) and a_c^{-1} (X_m, Y_m).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

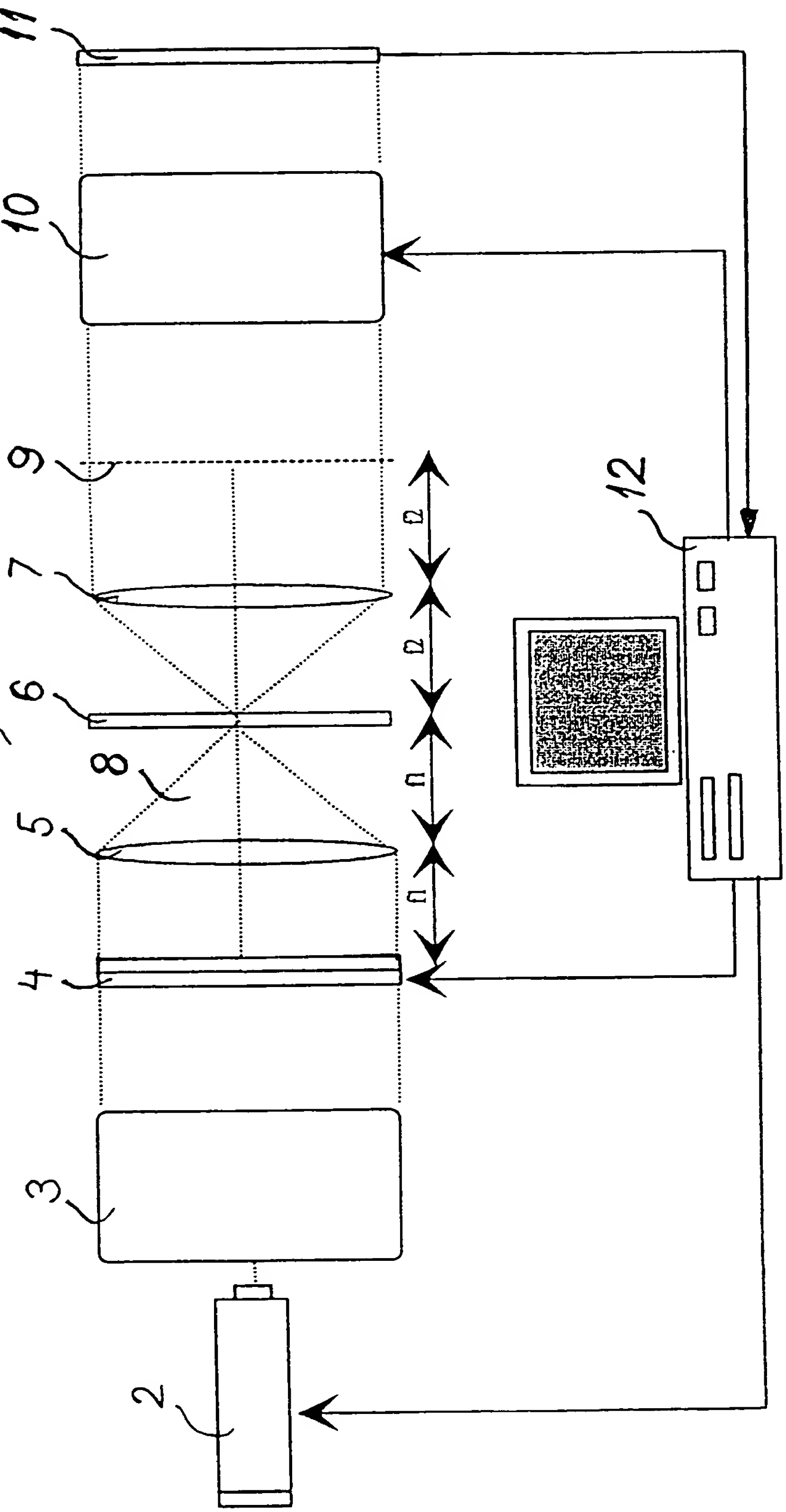


Fig. 1

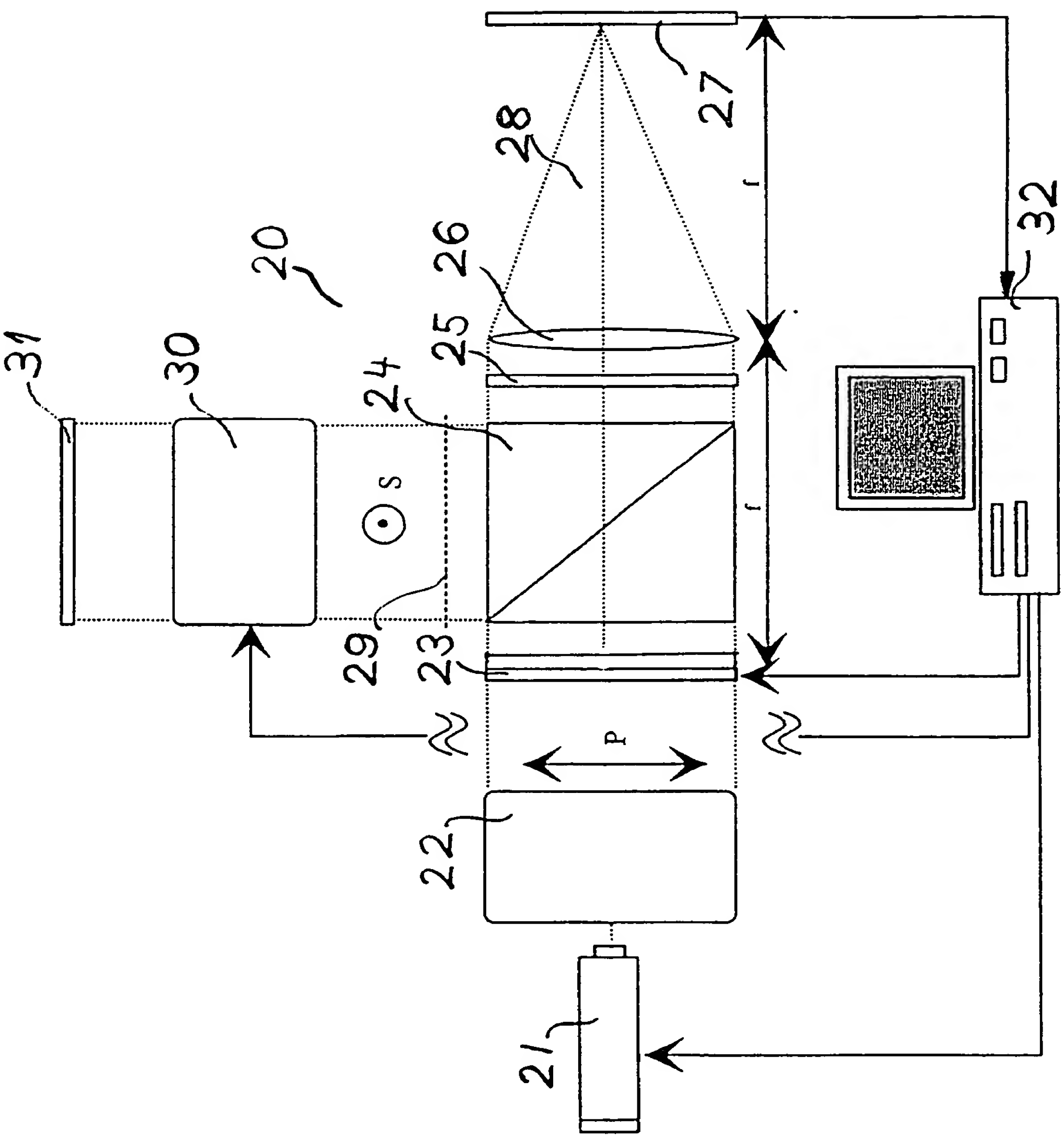


Fig. 2

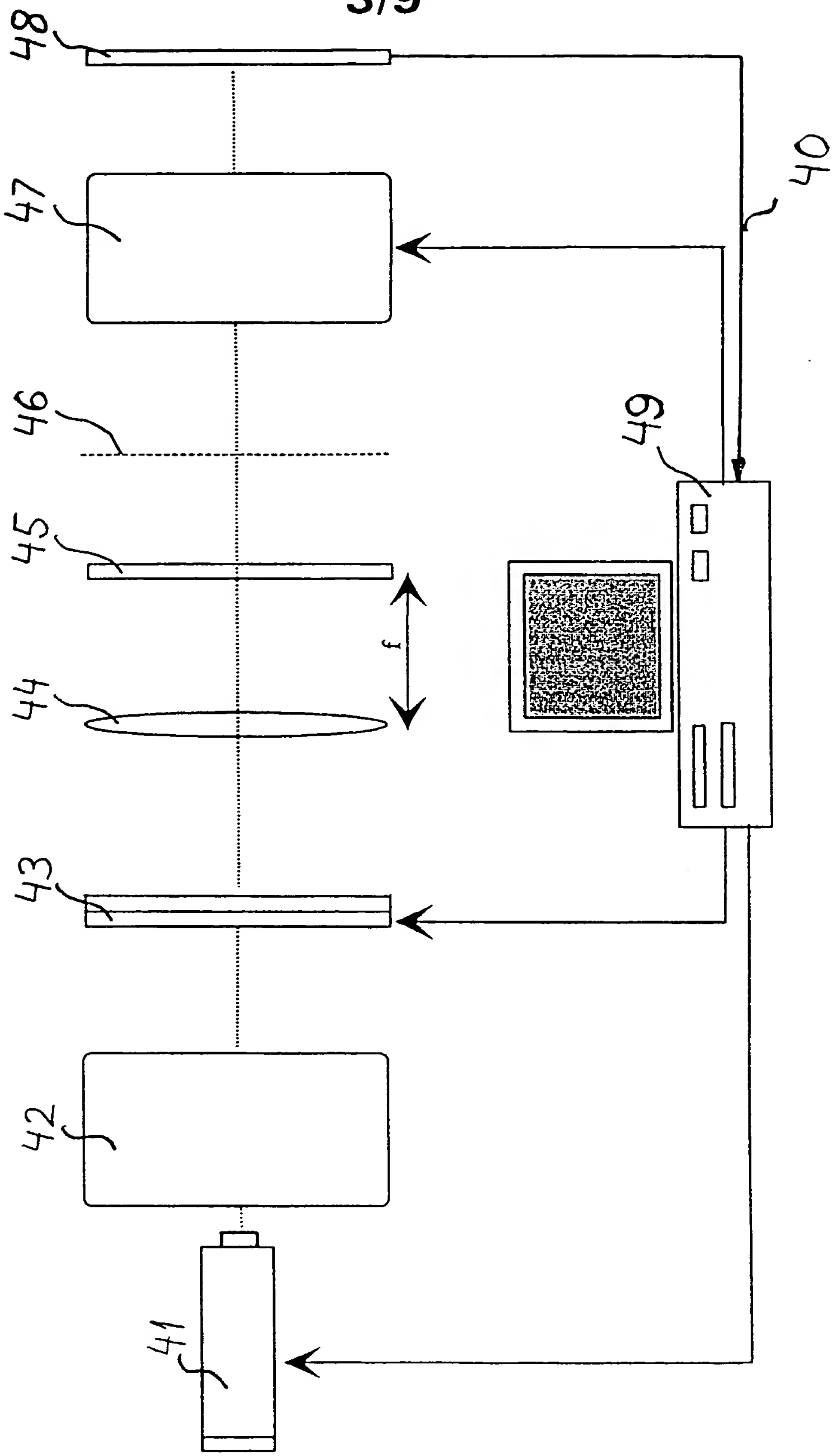


Fig. 3

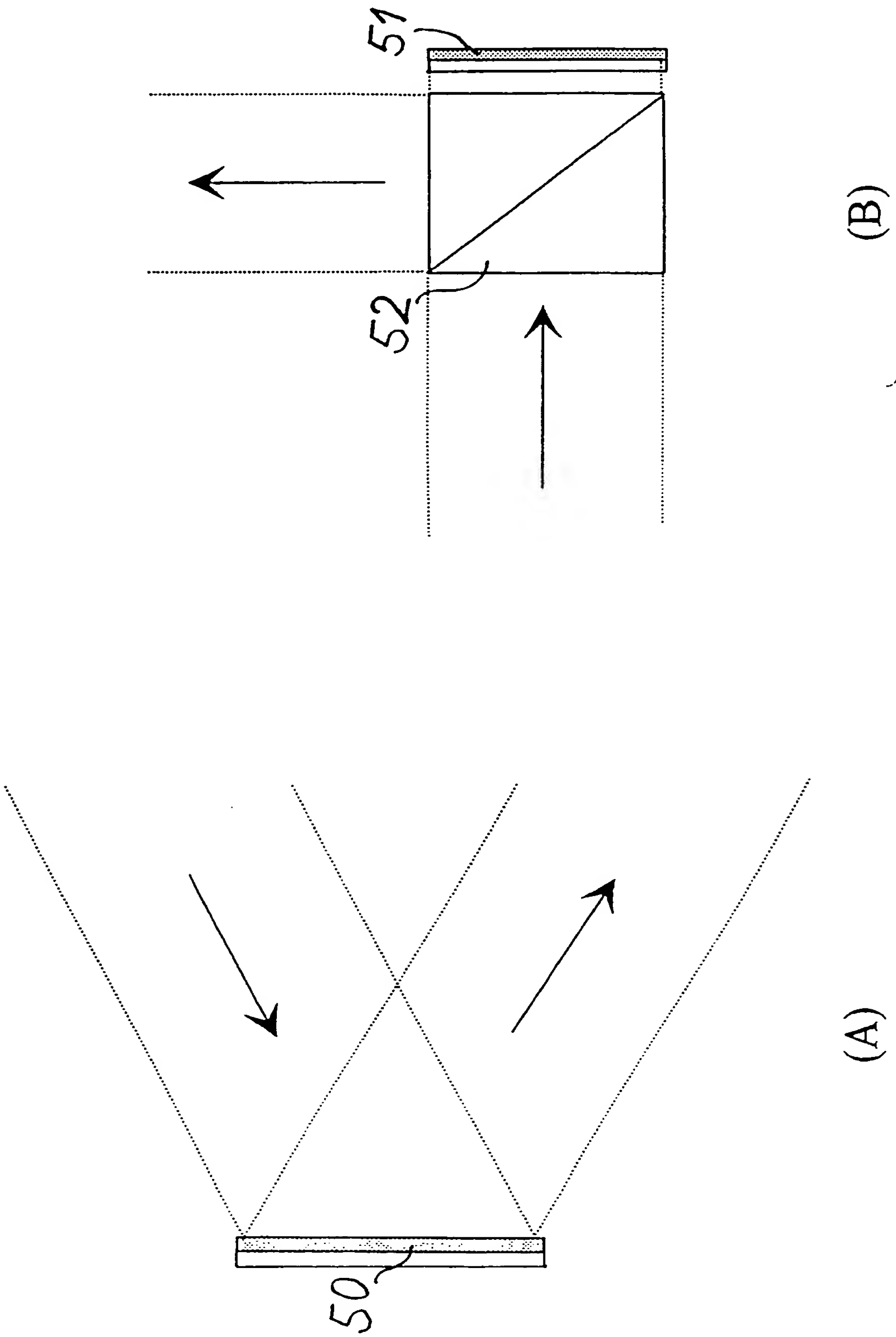


Fig. 4

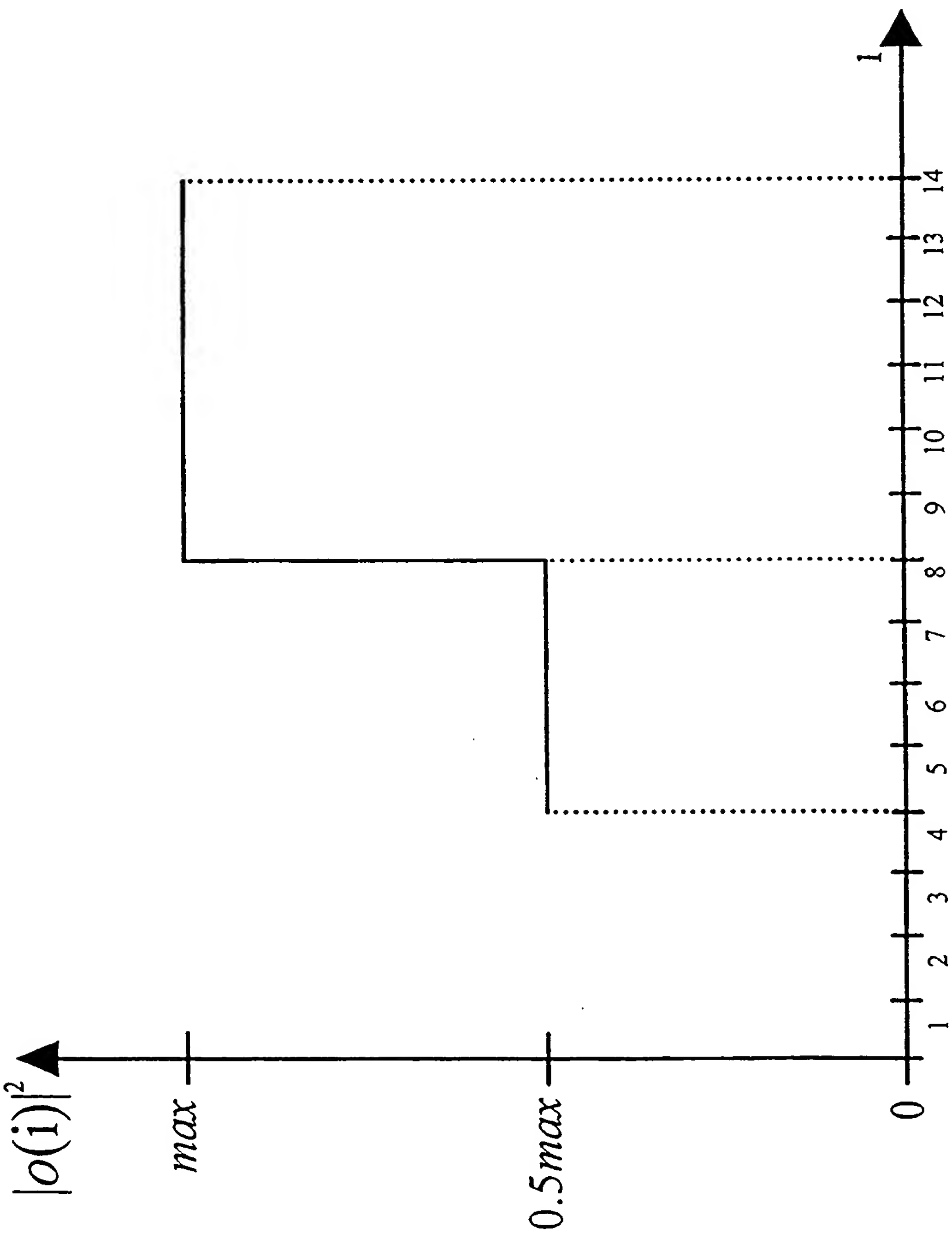


Fig. 5

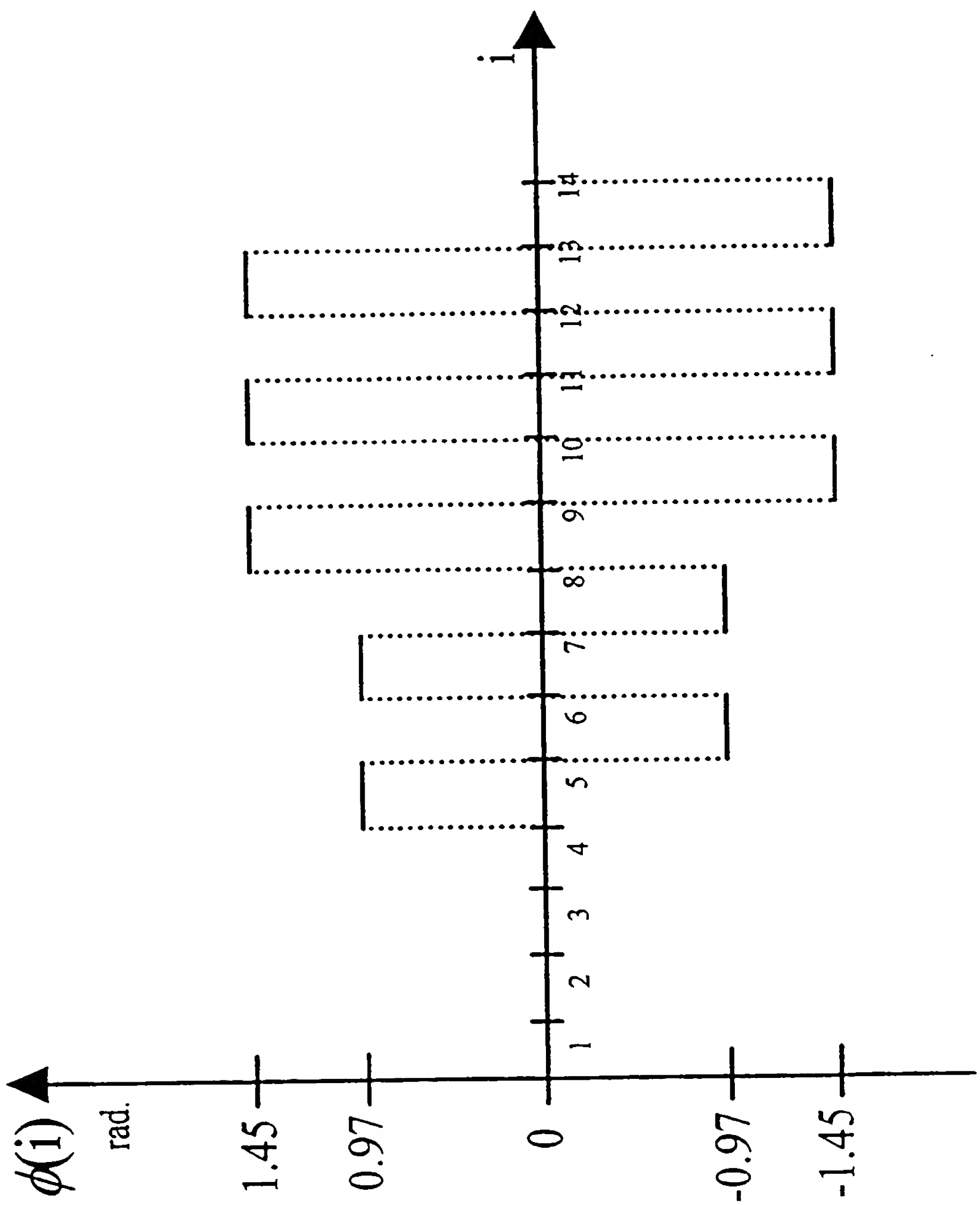
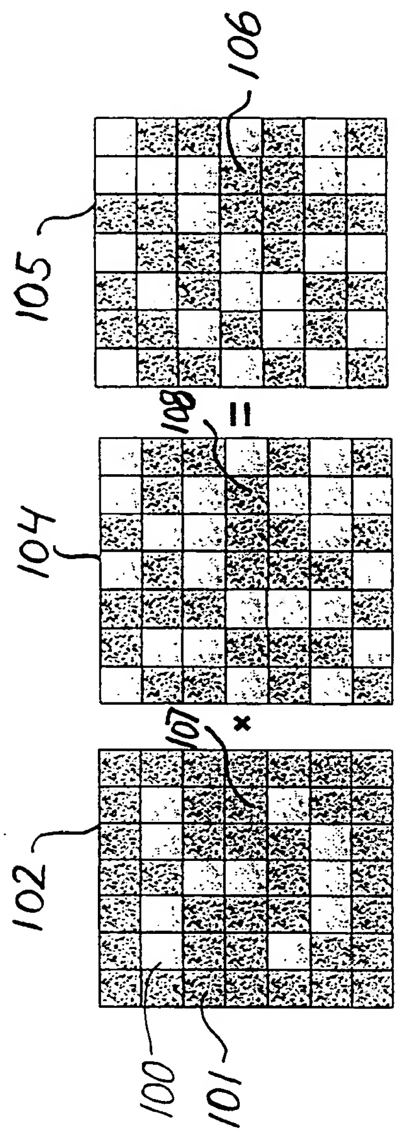


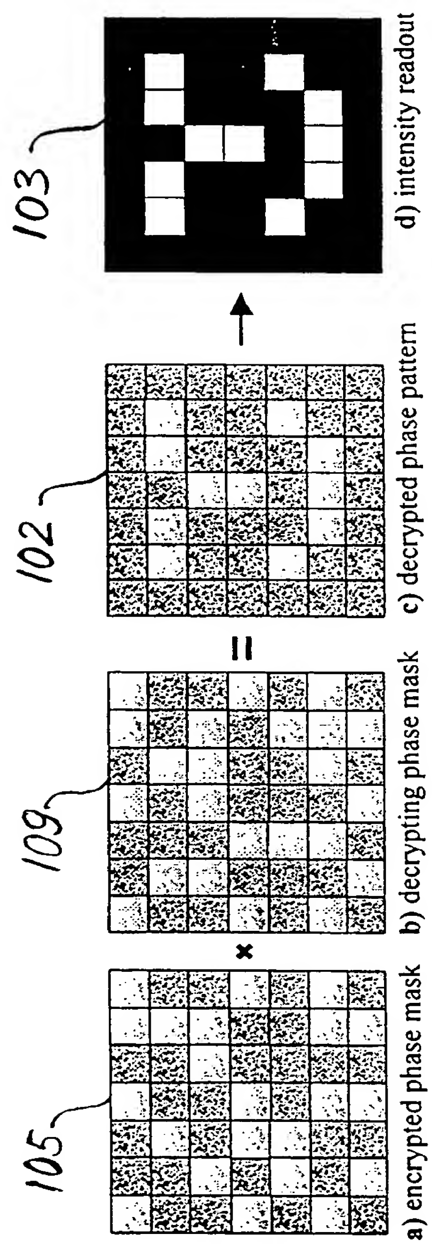
Fig. 6



a) encoded phase pattern b) encrypting phase pattern c) encrypted phase mask

Encryption Process for a binary phase image. The phase value of the pixels is either 0 (shown as light grey areas) or π (dark grey). The resulting phase mask (c) is a uniform random distribution of binary phase values and is generated by a multiplication of patterns (a) and (b) within the computer.

Fig. 7



The decryption process. This process is the reverse of that shown in Fig. 1, but is carried out optically, the high contrast image (d) is obtained using a π phase contrast filter in the decryption optics.

Fig. 8

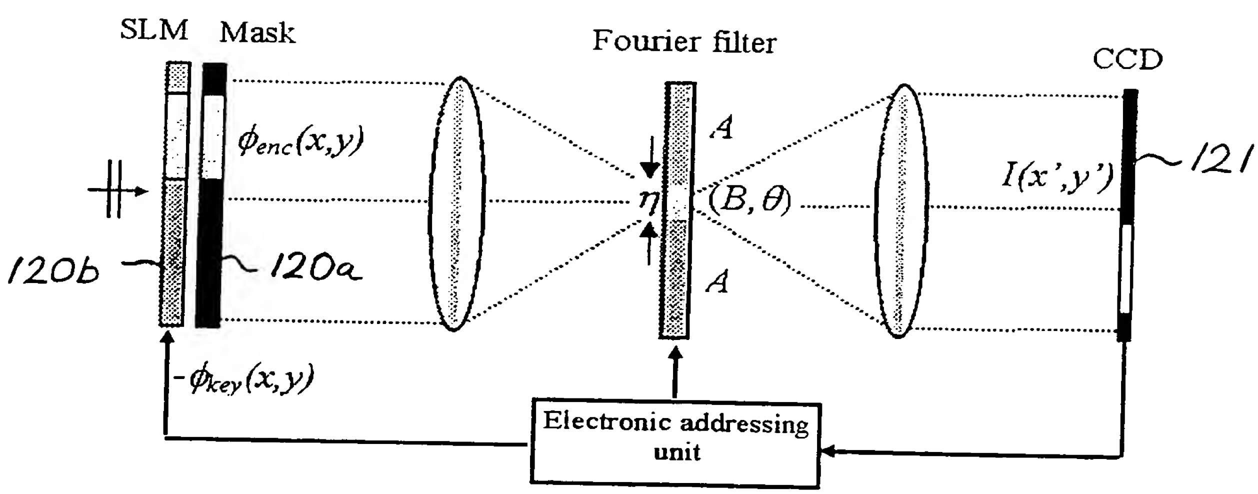

SLM
Mask
Fourier filter
CCD
$\phi_{enc}(x,y)$
A
η
(B,θ)
A
$I(x',y')$
121
120b
120a
$-\phi_{key}(x,y)$
Electronic addressing unit

Fig. 9

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DK 99/00331

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04K1/00 G02B27/52 G02B27/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04K G02B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JAVIDI: PHYSICS TODAY, vol. 50, no. 3, March 1997 (1997-03), pages 27-32, XP002116193 AMERICAN INSTITUTE OF PHYSICS, NEW YORK., US ISSN: 0031-9228 cited in the application page 30 -page 31; figure 4 ---	1,4,14, 28,31, 41,42,47
A	PATENT ABSTRACTS OF JAPAN vol. 016, no. 281 (P-1375), 23 June 1992 (1992-06-23) & JP 04 073790 A (NIPPON TELEGR & TELEPH CORP), 9 March 1992 (1992-03-09) abstract ---	1,11,28, 37

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 September 1999	06/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	von Moers, F

2

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 148 316 A (HORNER JOSEPH L ET AL) 15 September 1992 (1992-09-15) column 2, line 41 - line 69; figure 1	1,11,28, 37
A	WO 96 34307 A (RISOE FORSKNINGSCENTER ;GLUECKSTAD JESPER (DK)) 31 October 1996 (1996-10-31) cited in the application page 9; figure 1	1,3,28, 30

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DK 99/00331

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 04073790 A	09-03-1992	NONE	
US 5148316 A	15-09-1992	NONE	
WO 9634307 A	31-10-1996	AU 5496396 A	18-11-1996
		EP 0830632 A	25-03-1998
		JP 11504129 T	06-04-1999

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04K 1/00, G02B 27/52, 27/46

A1

(11) International Publication Number: WO 00/02339

(43) International Publication Date: 13 January 2000 (13.01.00)

(21) International Application Number: PCT/DK99/00331

(22) International Filing Date: 16 June 1999 (16.06.99)

(30) Priority Data:

PA 1998 00869	3 July 1998 (03.07.98)	DK
PA 1999 00364	15 March 1999 (15.03.99)	DK

(71) Applicant (*for all designated States except US*): FORSKNINGSCENTER RISØ [DK/DK]; Frederiksborgvej 399, P.O. Box 49, DK-4000 Roskilde (DK).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): GLÜCKSTAD, Jesper [DK/DK]; Voldumvej 45, st. tv, DK-2610 Rødovre (DK).

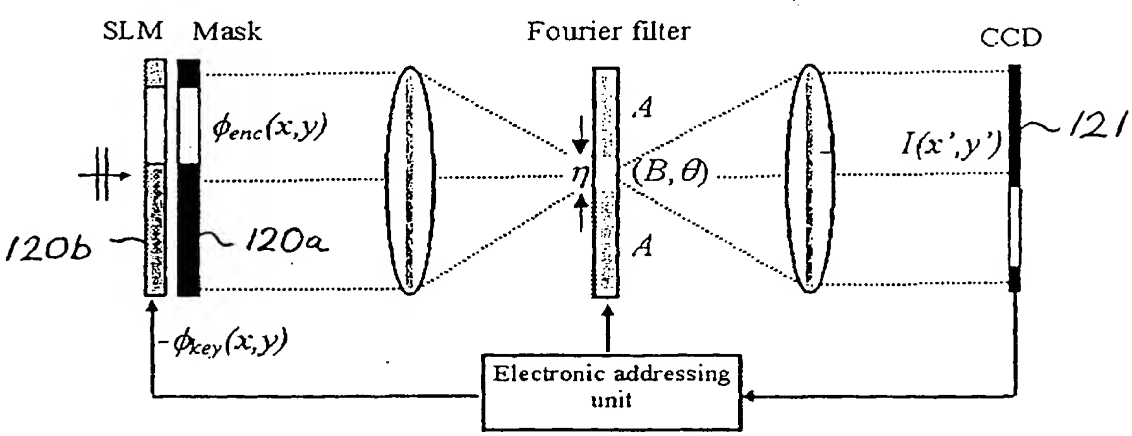
(74) Agent: PLOUGMANN, VINGTOFT & PARTNERS A/S; Sankt Annae Plads 11, P.O. Box 3007, DK-1021 Copenhagen K (DK).

(81) Designated States: AE, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

(54) Title: AN OPTICAL ENCRYPTION AND DECRYPTION METHOD AND SYSTEM



(57) Abstract

The invention relates to securing of information utilising optical imaging technologies and more specifically to phase encryption and decryption of images. An image is encrypted into a mask having a plurality of mask resolution elements (X_m, Y_m) by encoding the image using e.g. a phase mask with an encoded phase value ϕ (X_m, Y_m) and an encoded amplitude value a (X_m, Y_m), and by further encrypting the mask (using e.g. a spatial light modulator) by addition of an encrypting phase value ϕ_c (X_m, Y_m) to the encoded phase value ϕ (X_m, Y_m) and by multiplication of an encrypting amplitude value a_c (X_m, Y_m) with the encoded phase value a (X_m, Y_m). The method of decrypting comprises the steps of decrypting the mask by radiating electromagnetic radiation towards the mask and inserting into the path of the electromagnetic radiation a complex spatial electromagnetic radiation modulator comprising modulator resolution elements, the decrypting phase value ϕ_d (X_d, Y_d) and the decrypting amplitude value a_d (X_d, Y_d) respectively, of a modulator resolution element (X_d, Y_d) being substantially equal to $-\phi_c$ (X_m, Y_m) and a_c^{-1} (X_m, Y_m).

AN OPTICAL ENCRYPTION AND DECRYPTION METHOD AND SYSTEM

FIELD OF THE INVENTION

The invention relates to securing of information utilising imaging technologies and more specifically to phase and amplitude encryption and decryption of images.

BACKGROUND OF THE INVENTION

It is well known to form an image by phase contrast imaging methods in which phase modulation of light is converted into intensity modulation. As opposed to intensity modulation, phase modulation does not involve loss of energy.

In published patent application no. WO 96/34307, which is hereby incorporated by reference, a phase contrast imaging method is disclosed for calculating phasor values of a phase mask for synthesising a desired intensity pattern.

In "Securing Information with Optical Technologies", Bahram Javidi, Physics Today, Vol. 50, No. 3, March 1997, pp 27-32, a method and system for optically securing information is proposed. An image is encrypted in a 4f-lens optical configuration (i.e. comprising two Fourier transforming lenses) by Fourier transforming the image and an input phase mask with a first lens of the 4f-lens system. A Fourier plane phase mask having phasor values $e^{ib(\alpha,\beta)}$ is positioned in the Fourier plane of the first lens and an encrypted image is formed with a second lens that Fourier transforms images in the Fourier plane of the first lens. The encrypted image is decrypted in a similar 4f-lens configuration in which another Fourier plane phase mask (the key) having phasor values $e^{-ib(\alpha,\beta)}$ is positioned in the Fourier plane of the first lens.

It is a disadvantage of the known cryptographic method that encrypting an image both in the object plane and the Fourier plane leads to generation of speckle patterns in the decrypted image thereby corrupting data having been encrypted.

It is another disadvantage of the known cryptographic method that extremely accurate three-dimensional positioning of the phase mask in the Fourier plane is required for successful encryption and decryption.

It is yet another disadvantage of the known cryptographic method that both amplitude and phase have to be recorded in the encrypted mask.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide an apparatus of the above kind which apparatus is robust, compact, and simple to design and relatively cheap to manufacture.

It is another object of the present invention to provide an improved method and apparatus without the above-mentioned disadvantages.

It is still another object of the present invention to provide an improved method and apparatus for optically securing data utilising phase contrast imaging.

According to a first aspect of the present invention, a method is provided of decryption of an encrypted image having a non-encrypted image intensity pattern $I(x',y')$.

According to a second aspect of the present invention, the image is encrypted into a mask having a plurality of mask resolution elements (x_m,y_m) by encoding the image into the mask with an encoded phase value $\phi(x_m,y_m)$ and an encoded amplitude value $a(x_m,y_m)$, and by encrypting the mask by addition of an encrypting phase value $\phi_c(x_m,y_m)$ to the encoded phase value $\phi(x_m,y_m)$ and by multiplication of an encrypting amplitude value $a_c(x_m,y_m)$ with the encoded amplitude value $a(x_m,y_m)$. Thus, each mask resolution element (x_m,y_m) modulates the phase and the amplitude of electromagnetic radiation incident upon it with the complex value $a(x_m,y_m)a_c(x_m,y_m)e^{i\phi(xm,ym)+i\phi c(xm,ym)}$.

The method of decryption comprises the steps of decrypting the mask by radiating electromagnetic radiation towards the mask, and inserting into the path of the electromagnetic radiation a complex spatial electromagnetic radiation modulator comprising modulator resolution elements (x_d,y_d), each modulator resolution element (x_d,y_d) modulating the phase and the amplitude of electromagnetic radiation incident upon it with a predetermined complex value $a_d(x_d,y_d)e^{i\phi d(xd,yd)}$, the decrypting phase value $\phi_d(x_d,y_d)$ and the decrypting amplitude value $a_d(x_d,y_d)$, respectively, of a modulator resolution element (x_d,y_d) being substantially equal to $-\phi_c(x_m,y_m)$ and $a_c^{-1}(x_m,y_m)$, respectively, of a corresponding

mask resolution element (x_m,y_m), and imaging the mask and the electromagnetic radiation modulator onto the image having the image intensity pattern $I(x',y')$.

Throughout the present description the combination of the mask and the electromagnetic radiation modulator is denoted an encoder.

According to a third aspect of the present invention, a decryption system is provided for decrypting an encrypted image having a non-encrypted image intensity pattern $I(x',y')$ that has been encoded into a mask having a plurality of mask resolution elements (x_m,y_m) with an encoded phase value $\phi(x_m,y_m)$ and an encoded amplitude value $a(x_m,y_m)$, and encrypted by addition of an encrypting phase value $\phi_c(x_m,y_m)$ to the encoded phase value $\phi(x_m,y_m)$ and by multiplication of an encrypting amplitude value $a_c(x_m,y_m)$ with the encoded amplitude value $a(x_m,y_m)$, each mask resolution element (x_m,y_m) modulating the phase and the amplitude of electromagnetic radiation incident upon it with the complex value $a(x_m,y_m)a_c(x_m,y_m)e^{i\phi(xm,ym)+i\phi c(xm,ym)}$.

The system comprises a source of electromagnetic radiation for emission of electromagnetic radiation for illumination of the mask, a complex spatial electromagnetic radiation modulator that is positioned in the path of the electromagnetic radiation and comprises modulator resolution elements (x_d,y_d), each modulator resolution element (x_d,y_d) modulating the phase and the amplitude of electromagnetic radiation incident upon it with a predetermined complex value $a_d(x_d,y_d)e^{i\phi d(xd,yd)}$. The decrypting phase value $\phi_d(x_d,y_d)$ and the decrypting amplitude value $a_d(x_d,y_d)$, respectively, of a modulator resolution element (x_d,y_d) are substantially equal to $-\phi_c(x_m,y_m)$ and $a_c^{-1}(x_m,y_m)$, respectively, of a corresponding mask resolution element (x_m,y_m).

Further, the system comprises an imaging system for imaging the mask and the electromagnetic radiation modulator onto the image having the image intensity pattern $I(x',y')$.

The complex spatial electromagnetic radiation modulator may be positioned anywhere in the path of the electromagnetic radiation. When the complex modulator is positioned adjacent to the mask, the encrypted mask is decrypted when the decrypting phase value $\phi_d(x_d,y_d)$ and the decrypting amplitude value $a_d(x_d,y_d)$, respectively, of a modulator resolution element (x_d,y_d) being substantially equal to $-\phi_c(x_m,y_m)$ and $a_c^{-1}(x_m,y_m)$,

respectively, of a corresponding optically aligned mask resolution element (x_m,y_m).The mask and the decrypting complex modulator are optically aligned when corresponding mask resolution elements (x_m,y_m) and complex modulator resolution elements (x_d,y_d) are imaged onto the same desired resolution element (x',y') of the image having the image intensity pattern I(x', y').

For example, the complex modulator may be physically positioned remotely from the mask and imaged onto the position of the mask whereby the complex modulator is virtually positioned adjacent to the mask. Thus, the complex modulator may be positioned virtually or physically in another position than adjacent to the mask still performing the decrypting function when the amplitude and phase values of the complex modulator are transformed accordingly, e.g. by a Fresnel propagator.

As already mentioned, the optically aligned combination of the mask and the decrypting complex modulator is denoted the encoder. The virtual mask resolution elements of the encoder are denoted (x,y) and thus for optically aligned resolution elements, each of resolution elements (x,y) and (x_m,y_m) and (x_d,y_d) is imaged onto the same image resolution element (x',y'). For example when the mask and the complex modulator are positioned adjacent each other:

$$(x,y) = (x_m,y_m) = (x_d,y_d).$$

It is an important advantage of the present invention that the encrypted image may selectively require recording in the mask of phase values or amplitude values or a combination thereof.

It is another advantage of the present invention that decryption is performed in a plane adjacent to the mask or an equivalent plane whereby generation of speckles in the decrypted image is suppressed.

It is yet another advantage of the present invention that there is no requirement of positioning a radiation modulator in the Fourier plane whereby an accurate three-dimensional positioning requirement is avoided.

It is still another advantage of the present invention that only a single key for encryption is required.

It is preferred to encode the non-encrypted image into a phase mask and encrypt the phase mask by adding encrypting phase values to the encoded phase values. An encrypted phase mask is extremely difficult - if not impossible - to replicate by counterfeiters. Further, phase masks may be readily produced while masks requiring recording of both amplitude and phase are extremely complicated to produce, typically requiring production of two masks to be accurately superpositioned. The same applies to the decrypting complex modulator.

The imaging may be performed with a common path interferometer, such as a phase contrast imaging system, a dark field imaging system, a field absorption imaging system, a point diffraction imaging system, a Smartt interferometer, a Schlieren interferometer, etc, and any combination hereof.

Thus, the imaging for reconstruction of the intensity pattern I(x',y') may comprise:

Spatial modulation of electromagnetic radiation with the encoder for modulation of the phase of the incident electromagnetic radiation by phasor values of individual resolution elements of the encoder, each phasor value $e^{i\phi(x,y)}$ being determined in such a way that

1) the values of the Fourier transformed phasors attains predetermined values for predetermined spatial frequencies, and
2) the phasor value of a specific resolution element of the encoder corresponds to a distinct intensity level of the image of the resolution element in the intensity pattern,

Spatial phase filtering of electromagnetic radiation with a spatial phase filter for phase shifting of a part of the electromagnetic radiation, and

Generating the intensity pattern I(x',y') by interference in the image plane of an imaging system between the part of the electromagnetic radiation that has been phase shifted by the phase filter and the remaining part of the electromagnetic radiation.

Preferably, the method of decryption further comprises the steps of, and the decryption system further comprises means for Fourier or Fresnel transforming electromagnetic radiation modulated by the mask and the complex spatial electromagnetic radiation modulator, Filtering the Fourier or Fresnel transformed electromagnetic radiation by, in a region of spatial frequencies comprising DC in the Fourier or Fresnel plane, phase shifting with a predetermined phase shift value θ the modulated electromagnetic radiation in relation to the remaining part of the electromagnetic radiation, and multiplying the amplitude of the modulated electromagnetic radiation with a constant B, and in a region of remaining spatial frequencies in the Fourier or Fresnel plane, multiplying the amplitude of the modulated electromagnetic radiation with a constant A, forming the intensity pattern by Fourier or Fresnel transforming, respectively, the phase shifted Fourier or Fresnel transformed modulated electromagnetic radiation, whereby each resolution element (x_m,y_m) of the mask is imaged on a corresponding resolution element (x',y') of the image, the filtering parameters A, B, θ substantially fulfilling the equation

$$I(x',y') = A^2|a(x',y')e^{i\phi(x',y')} + \overline{\alpha}\,(BA^{-1}e^{i\theta}-1)|^2$$

$\overline{\alpha}$ being the average of the complex phasors $a(x,y)e^{i\phi(x,y)}$ of the encoder.

It should be noted that, in each resolution element of the encoder, one of two phasor values which represent a particular grey level of the intensity pattern I(x',y') may be selected.

It is further preferred that the filtering parameters A and B substantially fulfil that A=1 and B=1.

Preferably, the absorption of the mask is substantially uniform.

It is also preferred that the phase shift value θ substantially fulfils the equation

$$|\overline{\alpha}| = \frac{1}{2|\sin\frac{\theta}{2}|}$$

and in this case

$$I(x',y') = 2\left[1 \mp \sin(\phi_{\bar{\alpha}} - \phi(x',y') + \frac{\theta}{2})\right]$$

For selected phase shift values ϕ, $\phi_{\bar{\alpha}}$ being the phase of $\bar{\alpha}$.

In a preferred embodiment of the present invention, the phase shift θ is substantially equal to π. According the previous equation $\theta = \pi$ leads to $|\bar{\alpha}| = ½$, and then the phasor values $e^{i\phi(x,y)}$ of the encoder may be calculated in accordance with

$$I(x',y') = 2(1-\cos(\phi(x',y')))$$

$$\iint_{encoder} \sin(\phi(x,y)dxdy = 0\,.$$

Although, the present methods of encryption and decryption are related to encoding in two spatial dimensions (planar encoding), the principles of the methods may be utilised for encoding in one to three spatial dimensions and/or in the temporal dimension.

The electromagnetic radiation may be of any frequency range of the electromagnetic spectrum, i.e. the gamma frequency range, the ultraviolet range, the visible range, the infrared range, the far infrared range, the X-ray range, the microwave range, the HF (high frequency) range, etc. The present invention is also applicable to particle radiation, such as electron radiation, neutron radiation, etc.

Preferably, the electromagnetic radiation is monochromatic or quasi-monochromatic so that the energy of the electromagnetic radiation is concentrated in a narrow frequency bandwidth. Since the intensity pattern is reconstructed by interference of two electromagnetic waves emitted from a common source of electromagnetic radiation, the phases of which have been changed differently, it is required that the frequency range of

the emitted electromagnetic radiation is sufficiently narrow to ensure that the two waves of electromagnetic radiation are coherent so that their superposition generates the desired intensity pattern. If the frequency range is too broad, the two waves will be incoherent and the phase information will be lost as superposition of non-coherent waves results in a summation of the intensities of the two waves. It is required that the difference between individual delays of electromagnetic radiation to be superpositioned is less than the wavelength of the radiation. This is a relaxed requirement that allows the electromagnetic radiation to be relatively broad-banded. For example in the visible range a Xe-lamp or a Hg-lamp can be used as a light source in a system according to the present invention with the advantage compared to a laser light source that speckle noise is reduced. The requirements of the spatial coherence of the electromagnetic radiation depend upon the space bandwidth product of the corresponding system and how close the required system performance is to the theoretically obtainable performance of the system.

Preferably, the electromagnetic radiation is generated by a coherent source of electromagnetic radiation, such as a laser, a maser, a phaselocked laser diode array, etc. However a high pressure arc lamp, such as a Hg lamp, a Xe lamp, etc, may also be used and even an incandescent lamp may be used as a source of electromagnetic radiation in a low performance system.

The encoder changes the phase of an electromagnetic wave incident upon it. The encoder may transmit or reflect the incident electromagnetic wave. The encoder is divided into a number of resolution elements, each of which modulates the incident electromagnetic wave by changing its phase by a specific predetermined value. The predetermined values are assigned to each resolution element in different ways depending upon the technology applied in the component. For example in spatial light modulators, each resolution element may be addressed either optically or electrically. The electrical addressing technique resembles the addressing technique of solid-state memories in that each resolution element can be addressed through electronic circuitry to receive a control signal corresponding to the phase change to be generated by the addressed resolution element. The optical addressing technique addresses each resolution element by pointing a light beam on it, the intensity of the light beam corresponding to the phase change to be generated by the resolution element illuminated by the light beam.

Spatial phase modulation may be realised utilising fixed phase masks, devices comprising liquid crystals and being based on liquid crystal display technology, dynamic mirror devices, digital micro-mirror arrays, deformable mirror devices, membrane spatial light modulators, laser diode arrays (integrated light source and phase modulator), smart pixel arrays, etc.

A spatial phase filter is typically a fixed phase mask, such as an optically flat glass plate coated with a dielectric layer at specific positions of the glass plate. However, the spatial phase modulators mentioned in the previous section may also be used for spatial phase filters.

The imaging system maps the phase modulating resolution elements of the encoder on the target surface of the reconstructed intensity pattern. It may comprise a 4f-lens configuration (two Fourier transforming lenses utilising transmission of light or one Fourier transforming lens utilising reflection of light) or a single imaging lens. However, any optical imaging system providing a filtering plane for the spatial phase filter may be applied in a phase contrast imaging system.

In the method of decryption according to the present invention, the reconstructed intensity pattern is generated by superposition of two electromagnetic waves in the image plane of the imaging system. The encoder changes the phase values of an electromagnetic wave incident upon it and the imaging system directs the electromagnetic wave with changed phases reflected from or transmitted through the encoder towards the spatial phase filter. The phase filter phase shifts a part of the electromagnetic radiation and the imaging system is adapted to superimpose in the image plane the phase shifted part of the electromagnetic radiation with the part of the electromagnetic radiation that is not phase shifted by the spatial phase filter.

According to a preferred embodiment of the invention, the encoder is positioned at the front focal plane of a lens while the spatial phase filter is positioned in the back focal plane of the lens, whereby a first electromagnetic field at the encoder is Fourier transformed by the lens into a second electromagnetic field at the phase filter. Thus, specific spatial frequencies of the first electromagnetic field will be transmitted through the spatial phase filter at specific positions of the phase filter. For instance, the energy of the electromagnetic radiation at

zero frequency (DC) is transmitted through the phase filter at the intersecting point of the Fourier plane and the optical axis of the lens also denoted the zero-order diffraction region.

It is presently preferred that the spatial phase filter is adapted to phase shift the DC-part of the electromagnetic radiation and to leave the remaining part of the electromagnetic radiation unchanged or, alternatively, to leave the DC-part of the electromagnetic radiation unchanged and to phase shift the remaining part of the electromagnetic radiation. The last alternative is preferred when the energy level of the DC-part of the electromagnetic radiation is so high that the phase shifting part of the phase filter will be destroyed by it. For example in laser cutting, the DC level of the laser beam can be so high that a phase shifting dot positioned at the intersecting point of the DC part of the laser beam at the phase filter would evaporate. It is also possible to block the electromagnetic radiation (no transmittance) in the zero-order diffraction region, however, the DC energy of the radiation is then lost.

Below, an expression that is valid for phase modulation of the intensity of the reconstructed intensity pattern as a function of the phasor values $e^{i\phi(x,y)}$ of the encoder, when the DC-part of the electromagnetic radiation is phase shifted, is deduced.

Electromagnetic radiation incident on the encoder can be described by a function A(x,y), where A(x,y) is a complex number (amplitude and phase) of the incident field on the resolution element (x,y) of the encoder. At the resolution element (x,y), the encoder modulates the phase of the incident radiation with a value $\phi(x,y)$ so that the field after reflection by or transmission through the encoder may be described by the function A(x,y) * $e^{i\phi(x,y)}$, $e^{i\phi(x,y)}$ being the phasor value of the resolution element (x,y) of the encoder. As A(x,y) preferably is a constant value over the entire surface of the encoder, the term is left out of the following equations for simplicity.

The expression of the electromagnetic radiation incident on the spatial phase filter may now be separated into an AC-term and a DC-term. If the DC-term of the field is denoted $\overline{\alpha}$, the AC-term of the field is given by the term $e^{i\overline{\alpha}(x,y)} - \overline{\alpha}$. Since the spatial phase filter changes the phase of the DC-part of the electromagnetic radiation by θ, the intensity of the reconstructed intensity pattern at the image plane of the imaging system is given by:

$$I(x',y') = \left| e^{i\phi(x',y')} + \overline{\alpha}\,(e^{i\theta}-1) \right|^2$$

wherein (x',y') is the co-ordinates of the image of the resolution element (x,y) of the encoder formed by the imaging system in the image plane.

It should be noted that the second term of the equation is a complex number that adds to the phasors $e^{i\phi(x,y)}$ of the encoder and may be interpreted as a contrast control parameter for the reconstructed intensity pattern I(x',y').

According to a preferred embodiment of the invention, the average value of the phasors is adjusted in order to control the range of intensity levels.

Instead of phase shifting the DC-part of the electromagnetic radiation, it is also possible to synthesise a prescribed intensity pattern by phase shifting other parts of the electromagnetic radiation by adapting the spatial phase filter to phase shift electromagnetic radiation incident upon one or more arbitrary regions of the phase filter and leaving the phase of the remaining part of the electromagnetic radiation unchanged and then superimposing the two parts of the electromagnetic radiation. The corresponding mathematics and the corresponding design procedures for the encoder and spatial phase filter will of course be more complicated than for the method described in the previous section.

A simple example of phase shifting a part of the electromagnetic radiation of a spatial frequency different from the zero frequency is provided by moving the DC-part of the electromagnetic radiation to another spatial frequency in the Fourier plane (identical to the plane of the spatial phase filter) utilising an optical component with an appropriate carrier frequency (i.e. a grating or a prism) or, preferably, encoding the function of a grating or a prism into the encoder, and adapting the spatial phase filter to change the phase of the electromagnetic radiation at this spatial frequency and to leave the phase of the remaining part of the electromagnetic radiation unchanged.

According to another preferred embodiment of the invention, the encoder is not positioned in the back focal plane of the lens but in the Fresnel region of the lens instead. In this case, the electromagnetic field at the phase filter will be given by a Fresnel transformation of the electromagnetic field at the encoder. This further complicates the mathematics and the design procedures, for example the term in equation (7) below has to be substituted by the

value of the Fresnel transformation at the point(s) of phase changes of the phase filter. However, the Fresnel transformation may be calculated from a Fourier transformation by multiplication of the phasor values of the encoder by a quadratic phase factor followed by a Fourier transformation.

It is an important aspect of the present invention that each intensity level of the reconstructed intensity pattern for each resolution element may be generated by at least two different phasor values of a resolution element of the encoder.

For example, when the spatial phase filter phase shifts the DC-part of the electromagnetic radiation, it will be shown later that, advantageously, the average $\overline{\alpha}$ of the phasors of the resolution elements of the encoder should be equal to ½ and the value of the phase shift θ should be equal to π. In this case, the intensity of the reconstructed image pattern at the image (x',y') of the resolution element (x,y) will be given by:

$$I(x', y') = 2(1 - \cos \phi(x',y'))$$

It is seen that complex conjugate phasors (values of ϕ of opposite sign) result in identical intensity levels I(x',y'). It can be shown that for any value of the modulus of the average of the phasors $|\overline{\alpha}|$ two phasors exist that will generate identical intensity levels of the reconstructed intensity pattern.

Further, if the spatial phase filter phase shifts parts of the electromagnetic radiation different from the DC-part, the phasor value that generates a specific intensity level will depend on the position of the resolution element in question, i.e. the phasor value and the position of the resolution element with that phasor value together define the intensity level at the image of the resolution element in the reconstructed intensity pattern. Still, it is true that for each resolution element of the encoder, each intensity level of the reconstructed intensity pattern may be represented by one of two different phasors of complementary phase values.

This freedom of being able to select, for each intensity level to be generated and for each resolution element of the encoder, one of two phasors is used to control the phase of the Fourier transform of the phasors at specific spatial frequencies by selection of phasors with

appropriate phase values to ensure two intervals of biunique functional dependence between phasor values and corresponding intensity values.

This freedom of choice of phasors may be utilised to select phasors of neighbouring resolution elements of the encoder with a maximum difference between them, thereby generating an electromagnetic radiation emitted from the encoder with a maximum content of high spatial frequencies which will generate a good separation of the DC part of the electromagnetic radiation from its AC part. However, any other strategy of selecting between two possible phasor values of each resolution element may be chosen to generate a desired spatial frequency content of the electromagnetic radiation.

Preferably, the phase of the Fourier transform of the phasors at specific spatial frequencies is adjusted in order to control whether the relation between each phasor and the corresponding intensity level is a monotonic increasing or a monotonic decreasing function.

Below, a set of different steps that may be incorporated - either alone or in combination - into the method of encryption is described. They are provided according to the present invention for adjustment of the modulus of the Fourier transform of the phasors at specific spatial frequencies to attain a prescribed value.
According to one of the steps, the individual phasors of the resolution elements of the encoder are adjusted by a constant value until the desired value of the modulus of the Fourier transform of the phasors at specific spatial frequencies is attained while maintaining prescribed relative intensity levels between intensities of resolution elements of the intensity pattern, i.e. iteratively.

According to another step, the individual phasors of the resolution elements of the encoder are adjusted utilising histogram techniques known from image processing. A histogram is a bar chart showing the number of resolution elements of the reconstructed intensity pattern with a specific intensity value as a function of the intensity value. Any histogram technique, such as histogram equalisation, adapting the histogram to a predetermined distribution, etc., may be used iteratively until the modulus of the Fourier transform of the phasors at specific spatial frequencies attain the prescribed value.

According to yet another step, the phasor pattern of the encoder is spatially scaled in order to adjust the modulus of the Fourier transform of the phasors at specific spatial frequencies.

According to still another step, the modulus of the Fourier transform of the phasors at specific spatial frequencies is adjusted utilising half tone coding techniques, such as raster techniques, area ratio modulation, spot diameter modulation, etc.

Each complex phasor $a(x,y)e^{i\phi(x,y)}$ of the encoder may be selected from a set of two determined phasors with complementary complex phasor values $a(x,y)e^{i\phi 1(x,y)}$ and $a(x,y)e^{i\phi 2(x,y)}$ in such a way that a specific spatial frequency distribution of the intensity of the electromagnetic radiation in the Fourier or Fresnel plane is attained.

The phase $\phi(x,y)$ of complex phasors $a(x,y)e^{i\phi(x,y)}$ of adjacent resolution elements may alternate between the two possible complementary complex phasor values $a(x,y)e^{i\phi 1(x,y)}$ and $a(x,y)e^{i\phi 2(x,y)}$.

The complex phasors $a(x,y)e^{i\phi 1(x,y)}$ and $a(x,y)e^{i\phi 2(x,y)}$ may be complex conjugated.

It is seen from the description above that the intensity levels may differ from one reconstructed intensity pattern to the next as a consequence of the adjustments of the modulus of the Fourier transform of the phasors at specific spatial frequencies. Thus, it is preferred to control the power of the radiation source in dependence of the intensity range of the intensity pattern so that a sequence of different intensity patterns shows uniform intensity levels.

According to a preferred embodiment of the invention, the shape of the phase filter is adapted to match the spatial frequency content of the phasors of the encoder, e.g. to optimise the desired separation of the part of the electromagnetic radiation to be phase filtered from the remaining part of the electromagnetic radiation.

It is within the scope of the present invention that the imaging system further comprises zooming means for variable scaling of the reconstructed intensity pattern. The zooming of the imaging system may be dynamically controllable, e.g. in response to the scaling of the pattern of phasor values of the encoder.

According to the present invention, the power of the radiation source may be controllable in response to the spatial scaling of the pattern in the encoder and/or the zooming of the focusing system.

In order to provide a compact and integrated system according to the present invention, the optical function of a Fourier-transforming lens is encoded into the phasors of the encoder. The Fourier transforming lens may be refractively or diffractively encoded.

Similarly, the optical function of an output lens may be encoded into the phase filter either refractively or diffractively.

Further, compensation may be encoded into the phasor values of the encoder so that part of the electromagnetic radiation modulated by the encoder has a substantially flat intensity profile in the image plane. Without this compensation, part of the electromagnetic radiation modulated by the encoder will have a flat profile with perturbations resulting from the phase filtering superpositioned upon it. This may cause "ringings" (oscillations) at the edges of the reconstructed intensity pattern.

According to another preferred embodiment of the invention, the source of electromagnetic radiation comprises one or more light sources of different wavelengths corresponding to three different colours, such as red, green and blue, for generation of intensity patterns of arbitrary colours. Further, several independent systems each one illuminated by its own wavelength can be combined into a single multi-wavelength system.

According to yet another preferred embodiment of the present invention, the phasor values of the resolution elements of the mask and the electromagnetic radiation modulator are binary, i.e. each phasor value is selected from a set constituted by two values, for example 1 and -1 (corresponding to phase values 0 and π, respectively). It is further preferred that the random distribution of the decrypting binary phasor values is uniform.

It is also preferred that the binary values are selected so that encryption and decryption correspond to a binary XOR logical operation since the XOR operation provides maximum ambiguity as to which inputs generate a specific output.

It is even more preferred that there is no spatial correlation between resolution elements in the encoded, non-encrypted phase pattern.

The reconstructed intensity pattern $I(x',y')$ may be detected by a camera, such as a CCD camera, and the recorded image may be transmitted to a computer for recognition of the image $I(x',y')$ and thus, authentication of the encrypted mask.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a 4f common path interferometer,

Fig. 2 shows a 2f common path interferometer,

Fig. 3 shows a 1f common path interferometer,

Fig. 4 shows (A) off-axis read-out of reflective SLM and (B) on-axis read-out of reflective SLM,

Fig. 5 shows schematically an example of a prescribed intensity pattern in 1D,

Fig. 6 shows schematically the resulting phase encoding corresponding to Fig. 5,

Fig. 7 illustrates a binary phase image encryption method according to the present invention,

Fig. 8 illustrates a binary phase image decryption method according to the present invention, and

Fig. 9 illustrates alignment of an encrypted phase mask and a decrypting phase mask.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Fig. 1 shows a 4f common path interferometer 1. A laser 2 emits a light beam which is expanded by a beam expander 3 into a plane light wave of uniform intensity and directs it towards an encoder 4, i.e. a combination of an encrypted mask 4a and a decrypting

complex spatial electromagnetic radiation modulator 4b. The light beam is transmitted through the encoder 4 and a Fourier transforming lens 5. The encoder 4 is positioned in the front focal plane of the lens 5 and a spatial filter 6 is positioned in the back focal plane of the lens 5 that is also the front focal plane of a lens 7. The Fourier transforming lenses 5, 7 need not have identical focal lengths. Different focal lengths lead to a magnification ratio different from one. The filter 6 phase shifts by θ and optionally attenuates (by a factor B) the zero order diffraction part 8 of the light modulated by the encoder 4. Optionally, the remaining diffraction part of the light modulated by the encoder 4 may be attenuated by a factor A. The reconstructed intensity pattern is generated in the back focal plane 9 of the lens 7 and a dynamic focusing system 10 images the reconstructed intensity pattern $I(x',y')$ onto a focusing plane 11. The reconstructed intensity pattern $I(x',y')$ may be detected by a camera, such as a CCD camera, and the recorded image may be transmitted to a computer 12 for recognition of the image $I(x',y')$ and thus, authentication of the encrypted mask 4a.

The computer 12 controls the optical system. The computer 12 comprises interface means for addressing each of the resolution elements of the complex spatial electromagnetic radiation modulator 4b and transmitting a decrypting value to the addressed resolution element. Alternatively, the complex spatial electromagnetic radiation modulator 4b may be a fixed mask i.e. a mask manufactured with fixed modulating values of the resolution elements.

Optionally, the phase shift θ and attenuation factors (A, B) of the filter 6 is adjustable and controllable by optional phase control means of the computer 12 which may be further adapted to adjust the phase shift, e.g. utilising equation 18.

Fig. 2 shows a 2f common path interferometer 20. A laser 21 emits a light beam which is expanded by a beam expander 22 into a plane light wave of uniform intensity and directs it towards an encoder 23, i.e. a combination of an encrypted mask 23a and a complex spatial electromagnetic radiation modulator 23b and a polarisation beam splitter 24 and a quarter-wave plate 25. The polarisation beam splitter 24 and the quarter-wave plate 25 allows beam-splitting of light of a specific linear polarisation without the power loss associated with conventional beam-splitters due to splitting of the beam in both directions of transmission through the beam-splitter. After transmission through the polarisation beam splitter 24 and the quarter-wave plate 25, the light beam is transmitted through a Fourier

transforming lens 26 and is reflected from a spatial filter 27. The encoder 23 is positioned in the front focal plane of the lens 26 and the spatial filter 27 is positioned in the back focal plane of the lens 26. The filter 27 phase shifts by θ and optionally attenuates (by a factor B) the zero order diffraction part 28 of the light modulated by the encoder 23. Optionally, the remaining diffraction part of the light modulated by the encoder 23 may be attenuated by a factor A. The reconstructed intensity pattern I(x',y') is generated in the back focal plane 29 of the lens 26 and a dynamic focusing system 30 images the reconstructed intensity pattern I(x',y') onto a focusing plane 31. As described for the system shown in Fig. 1, the image I(x',y') may be detected with a camera and transmitted to a computer 32 for processing and authentication and the system 20 may also be controlled by the computer 32.

Fig. 3 shows a 1f common path interferometer 40. A laser 41 emits a light beam which is expanded by a beam expander 42 into a plane light wave of uniform intensity and directs it towards an encoder 43, i.e. a combination of an encrypted mask 43a and a complex spatial electromagnetic radiation modulator 43b. The light beam is transmitted through the encoder 43 and an image forming lens 44. The filter 45 phase shifts by θ and optionally attenuates (by a factor B) the zero order diffraction part of the light modulated by the encoder 43. Optionally, the remaining diffraction part of the light modulated by the encoder 43 may be attenuated by a factor A. The reconstructed intensity pattern is generated in the image plane 46 of the lens 44 and a dynamic focusing system 47 images the reconstructed intensity pattern I(x',y') onto a focusing plane 48. As described for the system shown in Fig. 1, the image I(x',y') may be detected with a camera and transmitted to a computer 49 for processing and authentication and the system 40 may also be controlled by the computer 49.

Fig. 4 shows details of (Fig. 4A) an off-axis read-out of an encoder 50 comprising a combination of a reflective mask 50a and a complex spatial electromagnetic radiation modulator 50b and of (Fig. 4B) an on-axis read-out of an encoder 51 comprising a combination of a reflective mask 51a and a complex spatial electromagnetic radiation modulator 51b with a beam splitter 52. Both configurations (Fig. 4A, Fig. 4B) may be utilised in the systems shown in Figs. 1-3.

PHASE ENCODING FOR DC PHASE FILTERING

In the following an example of encoding an encoder and a spatial phase filter will be given based on a system filtering in the DC-frequency range. The exemplified system is based on a 4-f lens configuration as shown in Fig. 1 and illuminated by electromagnetic radiation in the visible frequency domain, hereafter simply denoted as *light* radiation.

Assuming that the illuminating light is monochromatic and has a substantially flat amplitude profile we obtain the following spatial amplitude distribution emitted from the encoder:

$$a(x, y) = \mathrm{rect}\left(\frac{x}{\Delta x}, \frac{y}{\Delta y}\right)\exp(i\phi(x, y)) \quad (1)$$

where $\alpha(x, y) = \exp(i\phi(x, y))$ represent the spatially encoded phasor values and $\Delta x \Delta y$ is the area of the input phase modulating spatial light modulator.

It turns out to be convenient to separate $\alpha(x, y)$ into two terms describing a spatially invariant DC-value, $\bar{\alpha}$, and a spatially varying AC-contribution $\Delta\alpha(x, y)$. The DC-value can be found as:

$$\bar{\alpha} = \frac{1}{\Delta x \Delta y} \iint_{\Delta x \Delta y} \exp(i\phi(x, y)) dx dy \quad (2)$$

Subsequently the AC-term is expressed by:

$$\Delta\alpha(x, y) = \exp(i\phi(x, y)) - \frac{1}{\Delta x \Delta y} \iint_{\Delta x \Delta y} \exp(i\phi(x, y)) dx dy \quad (3)$$

The separation of $\alpha(x, y)$ into a spatially invariant DC-term and a spatially varying AC-term is an important point and will be used throughout the remaining part of this example, especially in the description of the spatial filtering procedure.

The spatial filter utilised in this example is chosen as a circular phase contrast filter (different transverse shapes can also be used) centred around origo in the spatial frequency domain, denoted by co-ordinates (f_x, f_y):

$$T(f_r) = 1 + (\exp(i\theta) - 1)\mathrm{circ}\left(\frac{f_r}{\Delta f_r}\right), \tag{4}$$

where $f_r = \sqrt{f_x^2 + f_y^2}$ denotes radial spatial frequency and Δf_r describes the size of the circular (circ) phase filter.

In the spatial frequency domain (the filtering plane) the Fourier transformation ($\Im$) of the spatially modulated light radiation from the encoder is present. The filtering operation on the Fourier transformed light radiation performed by the spatial phase contrast filter can be expressed as a simple point-by-point multiplication procedure. Subsequently the spatially filtered light is inverse Fourier transformed ($\Im^{-1}$) by the second Fourier lens (Fourier transformation and reflected output co-ordinates) and the resulting spatial amplitude distribution in the image plane (with co-ordinates (x', y')) can accordingly be written as:

$$\begin{aligned} o(x', y') &= a(x', y') + (\exp(i\theta) - 1)\Im^{-1}\left(\Im(a(x, y))\mathrm{circ}\left(\frac{f_r}{\Delta f_r}\right)\right) \\ &\cong a(x', y') + \bar{\alpha}(\exp(i\theta) - 1)\mathrm{rect}\left(\frac{x'}{\Delta x}, \frac{y'}{\Delta y}\right) \\ &= [\exp(i\phi(x', y')) + \bar{\alpha}(\exp(i\theta) - 1)]\mathrm{rect}\left(\frac{x'}{\Delta x}, \frac{y'}{\Delta y}\right) \end{aligned} \tag{5}$$

Within the illumination-region, $(x', y') \in \Re'$, outlined by $\mathrm{rect}\left(\frac{x'}{\Delta x}, \frac{y'}{\Delta y}\right)$, one obtains:

$$|o(x', y')|^2 \cong 1 + 4|\bar{\alpha}| \sin\left(\frac{\theta}{2}\right)\left[|\bar{\alpha}| \sin\left(\frac{\theta}{2}\right) - \sin\left(\phi_{\bar{\alpha}} - \phi(x', y') + \frac{\theta}{2}\right)\right] \tag{6}$$

Requiring that $|o(x_o', y_o')|^2 \equiv 0$ corresponding to complete darkness as the lowest intensity level in regions $(x_o', y_o') \in \Re_o'$ implies:

$$1 + 4|\bar{\alpha}| \sin\left(\frac{\theta}{2}\right)\left[|\bar{\alpha}| \sin\left(\frac{\theta}{2}\right) - \sin\left(\phi_{\bar{\alpha}} - \phi_o + \frac{\theta}{2}\right)\right] = 0 \qquad (7)$$

where the abbreviation $\phi_o = \phi(x_o', y_o')$ has been used.

The solutions to Eq. (7) are given by:

$$|\bar{\alpha}| = \frac{\sin\left(\phi_{\bar{\alpha}} - \phi_o + \frac{\theta}{2}\right) \pm \sqrt{\sin^2\left(\phi_{\bar{\alpha}} - \phi_o + \frac{\theta}{2}\right) - 1}}{2\sin\left(\frac{\theta}{2}\right)} \qquad (8)$$

The requirement $0 < |\bar{\alpha}| < 1$ implies that:

$$\begin{aligned} &\sin^2\left(\phi_{\bar{\alpha}} - \phi_o + \frac{\theta}{2}\right) = 1 \Rightarrow \\ &\theta = \pi - 2(\phi_{\bar{\alpha}} - \phi_o) + p2\pi, \qquad p = 0, \pm1, \pm2, \ldots \end{aligned} \qquad (9)$$

leading to

$$|\bar{\alpha}| = \frac{\pm 1}{2\sin\left(\frac{\theta}{2}\right)} \Rightarrow \frac{1}{2} \leq |\bar{\alpha}| < 1 \qquad (10)$$

where the +sign is for θ -values in the interval:

$$\theta \in \left]\frac{\pi}{3}; \frac{5\pi}{3}\right[+ p_{even}2\pi \qquad (11)$$

and the -sign is for θ -values:

$$\theta \in \left]\frac{\pi}{3};\frac{5\pi}{3}\right[+ p_{odd}2\pi \tag{12}$$

The corresponding interval for $(\phi_{\bar{\alpha}} - \phi_o)$ is:

$$(\phi_{\bar{\alpha}} - \phi_o) \in \left]\frac{\pi}{3};-\frac{\pi}{3}\right[\tag{13}$$

Inserting the expression for $|\bar{\alpha}|$, one obtains the simple intensity expression:

$$|o(x',y')|^2 = 2\left[1 \mp \sin\left(\phi_{\bar{\alpha}} - \phi(x',y') + \frac{\theta}{2}\right)\right] \tag{14}$$

where

$$\iint_{\Delta x\Delta y} \exp(i\phi(x,y))dxdy = \Delta x\Delta y|\bar{\alpha}|\exp(i\phi_{\bar{\alpha}}) \tag{15}$$

The phase-only transformations imply that energy is conserved:

$$\iint_{\Delta x\Delta y} |o(x',y')|^2 dx'dy' = \iint_{\Delta x\Delta y} |a(x,y)|^2 dxdy = \Delta x\Delta y \tag{16}$$

A special case:

The most convenient choice for $\bar{\alpha}$ is: $\bar{\alpha} = \frac{1}{2}$ (implying that $\theta = \pi + p_{even}2\pi$), so that the output intensity can be described as:

$$|o(x',y')|^2 = 2[1 - \cos(\phi(x',y'))] \tag{17}$$

In this case the phase→intensity mapping is described by the intervals $[0;\pi] \rightarrow [0;4]$. By setting $\bar{\alpha} = \frac{1}{2}$ one obtains the following requirement to the phase function $\phi(x,y)$:

$$\begin{cases} \iint\limits_{\Delta x \Delta y} \cos(\phi(x, y))dxdy = \dfrac{\Delta x \Delta y}{2} \\ \iint\limits_{\Delta x \Delta y} \sin(\phi(x, y))dxdy = 0 \end{cases} \tag{18}$$

Inserting the expression for $|o(x', y')|^2$ in Eq. (16) yields:

$$2 \iint\limits_{\Delta x \Delta y} [1 - \cos(\phi(x', y'))]dx'dy' = \Delta x \Delta y \tag{19}$$

in accordance with the first of the integral expressions in Eq. (18).

Encoding procedure:

- A given intensity distribution (image) $|o(x', y')|^2$ is desired at the output side of the optical set-up.

- Pixellation of the image, that is generally represented in the greyscale range: $[0; gmax]$, provides the relation:

  $$\iint |o(x', y')|^2 dx'dy' = \Delta x \Delta y \Rightarrow \sum_{ij} |o(i, j)|^2 = \frac{gmax}{4} \# \, pix_{(\Delta x \Delta y)}.$$

- The histogram for the desired image $|o(i, j)|^2$ is adjusted (adj.) within the greyscale range $[0; gmax]$, so that the previous point is fulfilled:

  $$|o(i, j)|^2 \rightarrow |o(i, j)|^2_{adj}.$$

- The phase values can now be calculated as:

  $$\phi(i, j) = \arccos\left(1 - \frac{2|o(i, j)|^2_{adj}}{gmax}\right).$$

- As before pixellation provides the relation:

$$\sum_{ij} \sin(\phi(i, j)) = 0 .$$

- The previous point can now be fulfilled by complex conjugating half the input pixels having the same phase value in the phase histogram.

- The phase conjugate phase flipping provides a valuable tool (an extra degree of freedom) for manipulating the spatial frequency content in order to optimise the separation of low and high frequency terms at the filter plane.

- The scheme is robust to constant phase errors across the input spatial phase modulator, since Eq. (14) is a function of the difference: $\phi_{\bar{\alpha}} - \phi(i, j)$, only. Furthermore, small variations in the individual pixel phase values do not introduce any detrimental effects because the average value $\bar{\alpha}$, is a result of a very large phasor sum.

- If the desired intensity distribution is too small to include all energy, that is, the histogram is scaled to maximum and the left hand side of Eq. (16) is still smaller than the right hand side, then the input phase object can be scaled until Eq. (16) is fulfilled. In order to obtain a scale invariant output intensity level a dynamic focusing system is needed. Similarly, intensity invariance can be obtained by controlling the radiated power from the light source. Alternatively, one can ignore the residual background illumination and obtain intensity levels with a gain factor of 9^- (background constant equal to 1^-) for narrow generally shaped line structures (e.g. Eq. (6)).

Example 1:

A very simple example illustrating the individual steps in the above procedure will be given below. To simplify the example it will be considered in one dimension only. The starting point for encoding the encoder in this example is based on the following parameters:

$$\begin{cases} \overline{\alpha} = 0.5 \\ \theta = \pi \\ \# \, pix_{(\Delta x)} = 14 \\ gmax = 4 \end{cases} \tag{20}$$

Consider the pixellated 3-step function shown in Fig. 5 to be reconstructed in the image plane as an intensity distribution. From the above choices of parameters one obtains the simple relation between phase values in the encoder and the image intensity values:

$$|o(i)|^2 = 2[1 - \cos(\phi(i))] \tag{21}$$

To proceed from here it necessary to calculate the accumulated intensity $\sum_i |o(i)|^2$ in the image to be reconstructed. The accumulated intensity is easily calculated from an image histogram where the x-axis represents grey level value and the y-axis represents the amount of pixels in the image at a given grey level value. By use of a histogram $\sum_i |o(i)|^2$ is simply found as the weighted sum of all grey level values (x-axis) multiplied by their pixel counting (y-axis). This describes, so to speak, the "weight" of the image. In this simple example histogram calculations are not needed since we only have 3 grey levels with well-defined separations.

The value for the accumulated intensity has to obey the equality:

$$\sum_i |o(i)|^2 = \frac{gmax}{4} \# \, pix_{(\Delta x)} = \# \, pix_{(\Delta x)} = 14 \tag{22}$$

From Fig. 5 we obtain:

$$\sum_i |o(i)|^2 = 4\text{pixels} \cdot 0 + 4\text{pixels} \cdot (0.5max) + 6\text{pixels} \cdot max = 8max \tag{23}$$

So that the value for *max* can be estimated to be:

$$max = \frac{7}{4} \tag{24}$$

The corresponding adjusted intensity levels, $|\alpha(i)|^2_{adj}$, are therefore: 7/4, 7/8 and 0. These values can now be utilised to calculate the phase values of the encoder from the relation:

$$\phi(i) = \arccos\left(1 - \frac{2|\alpha(i)|^2_{adj}}{gmax}\right) = \arccos\left(1 - \frac{|\alpha(i)|^2_{adj}}{2}\right) \tag{25}$$

where from we obtain the three phase values: 1.45 rad. 0.97 rad. and 0 rad.

The last step needed in order to encode the encoder is that the following equality is fulfilled:

$$\sum_i \sin(\phi(i)) = 0 \tag{26}$$

Since we have the choice to use complex conjugate phasor values (two phasors giving the same intensity level) many approaches can be taken from here. A simple approach is to flip every second phasor with its complex conjugate value as shown in Fig. 6. The final phase values used in the encoder are accordingly: ± 1.45 rad. ± 0.97 rad. and 0 rad.

As the last step we can check whether the criteria: $\bar{\alpha} = 1 / 2$, is actually fulfilled with the chosen phasor encoding:

$$\bar{\alpha} = \frac{1}{14}(4\exp(i0) + 2\exp(i0.97) + 3\exp(i1.45) + 2\exp(-i0.97) + 3\exp(-i1.45)) \equiv 1 / 2 \tag{27}$$

GENERAL PHASE CORRECTION PROCEDURE INTEGRATED WITH THE PHASE ENCODING

In Eq. (6) we obtained an analytic relation between the phase values in the encoder and the resulting intensity distribution, within the region $(x', y') \in \Re'$:

$$|o(x', y')|^2 \cong 1 + 4|\bar{\alpha}|\sin\left(\frac{\theta}{2}\right)\left[|\bar{\alpha}|\sin\left(\frac{\theta}{2}\right) - \sin\left(\phi_{\bar{\alpha}} - \phi(x', y') + \frac{\theta}{2}\right)\right] \quad (28)$$

The analysis leading to the above relation was based on the assumption that $|\bar{\alpha}|$ is a constant value within the $\Re'$-domain. In other words, the following approximation was applied:

$$\Im^{-1}\left(\Im(a(x, y))\mathrm{circ}\left(\frac{f_r}{\Delta f_r}\right)\right) \cong \bar{\alpha}\mathrm{rect}\left(\frac{x'}{\Delta x}, \frac{y'}{\Delta y}\right) \quad (29)$$

However, for certain spatial filter parameters the left-hand side of this expression will not be a space invariant constant value throughout the whole $\Re'$-domain but will instead manifest slowly variations/oscillations. This will introduce small errors in the final superposition between the phase filtered DC-value and the direct propagated AC-signal. In order to circumvent this problem a technique is needed that can counteract the distortions by use of phase-only encoding in the components already present in the system. In what follows a procedure for integrating pre-distortion that counteracts the above mentioned distortions will be described that is purely based on modifying the phasor values in the encoder at the input side of the system. The method can also counteract other types of distortions inherent in a practical implementation of the system. Furthermore, the method can be applied in systems filtering at other spatial frequencies than DC.

Procedure:

When encoding the input phase function it is helpful to have a 'reverse' equation, expressing the input phase distribution as a function of an adjusted (electronic) image grey-level distribution, I_{slm}, addressing the input spatial light modulator:

$$\frac{4I_{slm}}{gmax} \cong 1 + 4|\bar{\alpha}(x', y')|\sin\left(\frac{\theta}{2}\right)\left[|\bar{\alpha}(x', y')|\sin\left(\frac{\theta}{2}\right) - \sin\left(\phi_{\bar{\alpha}}(x', y') - \phi(x', y') + \frac{\theta}{2}\right)\right] \quad (30)$$

where it has been taken into account that $\bar{\alpha}(x', y')$ is not considered as a constant but manifests a smooth oscillating behaviour within the optical image domain. The maximum value of I_{slm} is denoted $gmax$.

Now, one can derive a formula for the 'grey-level correction' $\Delta I_{slm}(x', y')$ that one needs to apply in order to encode a phase function that compensates for the spatial variation of the average phase value $\overline{\alpha}(x', y')$:

$$\begin{cases} \dfrac{4I_{slm}(x', y')}{gmax} \cong 1 + 4\left|\overline{\alpha}(x', y')\right| \sin\left(\dfrac{\theta}{2}\right)\left[\left|\overline{\alpha}(x', y')\right| \sin\left(\dfrac{\theta}{2}\right) - \sin\left(\phi_{\overline{\alpha}}(x', y') - \phi(x', y') + \dfrac{\theta}{2}\right)\right] \\ \phi(x', y') = \operatorname{acos}\left(1 - \dfrac{2(I_{slm}(x', y') + \Delta I_{slm}(x', y'))}{gmax}\right) \end{cases} \tag{31}$$

where the second relation has been derived from the first by setting $\overline{\alpha} = \dfrac{1}{2}$ and $\theta = \pi$.

By inserting the second relation in the first expression one gets:

$$\Delta I_{slm}(x', y') = \left(\frac{1}{2\left|\overline{\alpha}(x', y')\right|} - 1\right) I_{slm}(x', y') - \frac{gmax}{2\left|\overline{\alpha}(x', y')\right|}\left(\left|\overline{\alpha}(x', y')\right| - \frac{1}{2}\right)^2 \tag{32}$$

This formula is however not directly useful because it is related to the histogram adjusted grey-level distribution denoted by I_{slm}.

One needs a formula that relates the above correction term to the 'original' input grey-level distribution $I(x, y)$ that has not been modified by histogram adjustments. This is important since the effect of the grey-level corrections also have to be incorporated in the procedure of histogram adjustments.

The histogram scaling gives:

$$I(x, y) = \frac{I_{\max}}{I_{slm,\max}} I_{slm}(x, y) \tag{33}$$

where $I_{\max}$ and $I_{slm,\max}$ are the maximum grey-level values occurring in the original and the adjusted electronic grey-level distributions respectively.

Similarly, one can apply this relation to the intensity correction term ΔI_{slm} and obtain:

$$\tilde{I}(x, y) = I(x, y) + \Delta I(x, y) = \frac{I_{\max}}{I_{slm,\max}}\left(I_{slm}(x, y) + \Delta I_{slm}(x, y)\right) \tag{34}$$

resulting in:

$$\tilde{I}(x, y) = \frac{1}{2|\bar{\alpha}(x, y)|}\left(I(x, y) - gmax\,\frac{I_{\max}}{I_{slm,\max}}\left(|\bar{\alpha}(x, y)| - \frac{1}{2}\right)^2\right) \tag{35}$$

In order to have 'enough dynamic range' in grey-levels for the correction term one can derive an inequality from the above relation by using the fact that $\tilde{I}_{\max} \leq gmax$:

$$\frac{1}{2|\bar{\alpha}_{\min}|}\left(I_{\max} - gmax\,\frac{I_{\max}}{I_{slm,\max}}\left(|\bar{\alpha}_{\min}| - \frac{1}{2}\right)^2\right) \leq gmax \tag{36}$$

or

$$I_{\max} \leq \frac{2|\bar{\alpha}_{\min}| \cdot gmax}{\left(1 - \frac{gmax}{I_{slm,\max}}\left(|\bar{\alpha}_{\min}| - \frac{1}{2}\right)^2\right)} \tag{37}$$

Since the first term is the dominating term in the expression for the intensity correction it will in practice be sufficient just to have the much simpler corrections:

$$\begin{cases} \tilde{I}(x, y) = \dfrac{I(x, y)}{2|\bar{\alpha}(x, y)|} \\ I_{\max} \leq 2|\bar{\alpha}_{\min}| \cdot gmax \end{cases} \tag{38}$$

BINARY PHASE IMAGE ENCRYPTION AND DECRYPTION METHOD

Fig. 7 illustrates a binary phase image encryption method and Fig. 8 illustrates a binary phase image decryption method according to the present invention. In the illustrated example the modulating phase values are 0 or π. In Figs. 7 and 8 bright resolution

elements 100 have the phase shift value 0 and the dark resolution elements 101 have the phase shift value π.

The encryption method comprises the steps of

1) calculating, according to the mathematical method described above and in WO 96/34307, the modulating phase values $(0,\pi)$ of the resolution elements forming a binary encoded phase pattern 102 that is imaged onto the intensity pattern 103, e.g. by one of the systems illustrated in Figs. 1-3,

2) generating a uniform random distribution 104 of binary phase values $(0,\pi)$,

3) forming an encrypted phase mask 105, 4a, 23a, 43a, 50a, 51a by adding, for each resolution element 106 of the encrypted mask 105, the calculated phase value 107 (0 or π) and the corresponding generated random phase value 108 (0 or π) of the resolution element, whereby a uniform random distribution of binary phase values $(0,\pi)$ is generated in the encrypted phase mask 105 encrypting the image 103, and

the decryption method comprises the step of reconstructing the image 103 by

4) adding the binary phase shift value $(0,\pi)$ of each resolution element of the encrypted phase mask 105 to a binary phase shift value $(0,\pi)$ of a corresponding resolution element of a decrypting phase mask 109, 4b, 23b, 43b, 50b, 51b with resolution elements having the respective calculated phase values 104, whereby the original encoded phase pattern 102 is reconstructed.

The decrypting step 4) may be performed by aligning the encrypted phase mask 105 and the decrypting phase mask 109 in one of the optical systems illustrated in Figs. 1-3, whereby the original image 103 is reconstructed, e.g. for detection by a camera and recognition by a computer.

It should be noted that in the above example, encrypting and decrypting phase values of corresponding resolution elements are identical.

Utilisation of 0 and π as the binary phase values provides a particular robust encryption and decryption approach with a low sensitivity to perturbations of the masks because of the relatively large phase difference between the binary values of the mask.

In the common path interferometer illustrated in Fig. 9, the decrypting mask 120b is a spatial light modulator with a modulating region that is larger than the encrypted phase mask 120a. Thus, the encrypted phase mask 120a and the decrypting mask 120b can be aligned electronically by appropriate control of the spatial light modulator 120b. For example, the encrypted mask may contain regions with non-encrypted patterns that are imaged onto the CCD detector array 121 for the purpose of alignment. The positions of the imaged alignment patterns are detected and the spatial light modulator 120b is subsequently controlled accordingly whereby the decrypting resolution elements of the light modulator 120b are aligned with the resolution elements of the encrypted phase mask 120a.

CLAIMS

1. A method of decryption of an encrypted image having a non-encrypted image intensity pattern $I(x',y')$ and

Encoded into a mask having a plurality of mask resolution elements (x_m,y_m) with an encoded phase value $\phi(x_m,y_m)$ and an encoded amplitude value $a(x_m,y_m)$, and

Encrypted by addition of an encrypting phase value $\phi_c(x_m,y_m)$ to the encoded phase values $\phi(x_m,y_m)$ and by multiplication of an encrypting amplitude value $a_c(x_m,y_m)$ with the encoded amplitude value $a(x_m,y_m)$,

Each mask resolution element (x_m,y_m) modulating the phase and the amplitude of electromagnetic radiation incident upon it with the complex value $a(x_m,y_m)a_c(x_m,y_m)e^{i\phi(xm,ym)+i\phi c(xm,ym)}$, and

The method comprising the steps of

Radiating electromagnetic radiation towards the mask,

Inserting into the path of the electromagnetic radiation a complex spatial electromagnetic radiation modulator comprising modulator resolution elements (x_d,y_d), each modulator resolution element (x_d,y_d) modulating the phase and the amplitude of electromagnetic radiation incident upon it with a predetermined complex value $a_d(x_d,y_d)e^{i\phi d(xd,yd)}$, the decrypting phase value $\phi_d(x_d,y_d)$ and the decrypting amplitude value $a_d(x_d,y_d)$, respectively, of a modulator resolution element (x_d,y_d) being substantially equal to $-\phi_c(x_m,y_m)$ and $a_c^{-1}(x_m,y_m)$, respectively, of a corresponding mask resolution element (x_m,y_m), and

Imaging the mask and the electromagnetic radiation modulator onto the image having the image intensity pattern $I(x',y')$.

2. A method according to claim 1, wherein the step of imaging comprises imaging with a common path interferometer.

3. A method according to claim 1 or 2, wherein the step of imaging comprises phase contrast imaging.

4. A method according to claim 2 or 3, further comprising the steps of

Fourier or Fresnel transforming electromagnetic radiation modulated by the mask and the complex spatial electromagnetic radiation modulator,

Filtering the Fourier or Fresnel transformed electromagnetic radiation by

In a region of spatial frequencies comprising DC in the Fourier or Fresnel plane,

Phase shifting with a predetermined phase shift value θ the modulated electromagnetic radiation in relation to the remaining part of the electromagnetic radiation, and

Multiplying the amplitude of the modulated electromagnetic radiation with a constant B, and

In a region of remaining spatial frequencies in the Fourier or Fresnel plane, multiplying the amplitude of the modulated electromagnetic radiation with a constant A,

Forming the intensity pattern by Fourier or Fresnel transforming, respectively, the phase shifted Fourier or Fresnel transformed modulated electromagnetic radiation, whereby each resolution element (x_m,y_m) of the mask is imaged on a corresponding resolution element (x',y') of the image,

The filtering parameters A, B, θ substantially fulfilling the equation

$$I(x',y') = A^2|a(x',y')e^{i\phi(x',y')} + \overline{\alpha}\,(BA^{-1}e^{i\theta}-1)|^2$$

$\overline{\alpha}$ being the average of the complex phasors $a(x,y)e^{i\phi(x,y)}$.

5. A method according to claim 4, wherein the filtering parameters A and B substantially fulfil that A=1 and B=1, and wherein the absorption of the mask is substantially uniform.

6. A method according to claim 5, wherein the phase shift value θ substantially fulfils the equation

$$|\bar{\alpha}| = \frac{1}{2|\sin\frac{\theta}{2}|}$$

7. A method according to claim 6, wherein the phase shift θ is substantially equal to π.

8. A method according to any of claims 3-7, further comprising the steps of

Moving the DC-part of the electromagnetic radiation to a second part of the Fourier or Fresnel plane, and

Phase shifting the Fourier or Fresnel transformed modulated electromagnetic radiation at the second part of the Fourier or Fresnel plane by θ in relation to the remaining part of the electromagnetic radiation.

9. A method according to claim 8, wherein the step of moving the DC-part of the electromagnetic radiation comprises utilisation of an optical component, such as a grating, a prism, etc, with an appropriate carrier frequency.

10. A method according to any of claims 3-9, further comprising the step of phase shifting at selected spatial frequencies constituting a region that is shaped to match the spatial frequency content of the phasors $e^{i\phi(x,y)}$.

11. A method according to any of claims 3-10, wherein the step of filtering comprises utilisation of a spatial light modulator.

12. A method according to any of claims 3-11, further comprising the step of encoding the optical function of an output lens into the filter.

13. A method according to any of claims 3-12, wherein the step of radiating electromagnetic radiation comprises radiation of electromagnetic radiation of different wavelengths corresponding to three different colours, such as red, green and blue, for generation of intensity patterns of arbitrary colours.

14. A method of encryption of an image having an intensity pattern $I(x',y')$ to be decrypted according to any of claims 1-13, comprising the steps of

Pixellating the intensity pattern $I(x',y')$ in accordance with the disposition of resolution elements (x_m,y_m) of a mask,

Encoding the mask with an encoded phase value $\phi(x_m,y_m)$ and an encoded amplitude value $a(x_m,y_m)$, and

Encrypting by addition of an encrypting phase value $\phi_c(x_m,y_m)$ to the encoded phase values $\phi(x_m,y_m)$ and by multiplication of an encrypting amplitude value $a_c(x_m,y_m)$ with the encoded amplitude value $a(x_m,y_m)$,

Each mask resolution element (x_m,y_m) modulating the phase and the amplitude of electromagnetic radiation incident upon it with the complex value $a(x_m,y_m)a_c(x_m,y_m)e^{i\phi(xm,ym)+i\phi c(xm,ym)}$.

15. A method according to claim 14, further comprising the step of calculating the complex phasor values $a(x,y)e^{i\phi(x,y)}$ of the encoder in accordance with

$$I(x',y') = A^2|a(x',y')e^{i\phi(x',y')} + \bar{\alpha}(BA^{-1}e^{i\theta}-1)|^2$$

For selected phase shift values θ, $\bar{\alpha}$ being the average of the complex phasors $a(x,y)e^{i\phi(x,y)}$,

Selecting, for each resolution element, one of two phasor values which represent a particular grey level.

16. A method according to claim 15, wherein the filtering parameters A and B substantially fulfil that A=1 and B=1, and wherein the absorption of the mask is substantially uniform.

17. A method according to claim 16, wherein the step of calculating the phasor values comprises

Setting the reconstructed intensity of at least one resolution element (x_0', y_0') of the intensity pattern to zero, and

Calculating the phasor values $e^{i\phi(x,y)}$ of the mask in accordance with

$$|\overline{\alpha}| = \frac{1}{2|\sin\frac{\theta}{2}|}$$

$$I(x',y') = 2\left[1 \mp \sin(\phi_{\overline{\alpha}} - \phi(x',y') + \frac{\theta}{2})\right]$$

For selected phase shift values ϕ, $\phi_{\overline{\alpha}}$ being the phase of $\overline{\alpha}$.

18. A method according to claim 17, further comprising the step of selecting the phase shift $\theta = \pi$, selecting $|\overline{\alpha}| = ½$, and calculating the phasor values $e^{i\phi(x,y)}$ of the encoder in accordance with

$$I(x',y') = 2(1-\cos(\phi(x',y')))$$

$$\iint_{encoder} \sin(\phi(x,y)dxdy = 0.$$

19. A method according to any of claims 14-18, further comprising the step of encoding the function of an optical component, such as a grating, a prism, etc, with an appropriate carrier frequency, into the mask.

20. A method according to any of claims 14-19, further comprising the step of adjusting the modulus of the Fourier transform of the complex phasors $a(x,y)e^{i\phi(x,y)}$ at specific spatial frequencies in order to control the range of intensity levels of the reconstructed intensity pattern.

21. A method according to claim 20, wherein the step of adjusting the modulus of the Fourier transform of the complex phasors $a(x,y)e^{i\phi(x,y)}$ at specific spatial frequencies comprises at least one of the following measures:

a) Adjusting the individual complex phasors $a(x,y)e^{i\phi(x,y)}$ of the resolution elements of the mask maintaining prescribed relative intensity levels between intensities of resolution elements of the intensity pattern,

b) Adjusting the individual complex phasors $a(x,y)e^{i\phi(x,y)}$ of the resolution elements of the mask by histogram techniques,

c) Spatially scaling the complex phasor $a(x,y)e^{i\phi(x,y)}$ pattern of the mask, and

d) Utilising half tone coding techniques.

22. A method according to any of claims 14-21, wherein each complex phasor $a(x,y)e^{i\phi(x,y)}$ of the mask is selected from a set of two determined phasors with complementary complex phasor values $a(x,y)e^{i\phi 1(x,y)}$ and $a(x,y)e^{i\phi 2(x,y)}$ in such a way that a specific spatial frequency distribution of the intensity of the electromagnetic radiation in the Fourier or Fresnel plane is attained.

23. A method according to claim 22, wherein the phase $\phi(x,y)$ of complex phasors $a(x,y)e^{i\phi(x,y)}$ of adjacent resolution elements alternates between the two possible complementary complex phasor values $a(x,y)e^{i\phi 1(x,y)}$ and $a(x,y)e^{i\phi 2(x,y)}$.

24. A method according to claim 22 or 23, wherein the complex phasors $a(x,y)e^{i\phi 1(x,y)}$ and $a(x,y)e^{i\phi 2(x,y)}$ are complex conjugated.

25. A method according to any of claims 14-24, further comprising the step of encoding the optical function of a Fourier-transforming lens into the complex phasors $a(x,y)e^{i\phi(x,y)}$ of the encoder.

26. A method according to any of claims 14-25, wherein each of the encrypting phase values $\phi_c(x_m,y_m)$ is substantially equal to a value selected from a set consisting of two phase values.

27. A method according to claims 26, wherein each of the encrypting phase values $\phi_c(x_m,y_m)$ is substantially equal to a value selected from the set consisting of 0 and π.

28. A decryption system for decrypting an encrypted image having a non-encrypted image intensity pattern $I(x',y')$ that has been

Encoded into a mask having a plurality of mask resolution elements (x_m,y_m) with an encoded phase value $\phi(x_m,y_m)$ and an encoded amplitude value $a(x_m,y_m)$, and

Encrypted by addition of an encrypting phase value $\phi_c(x_m,y_m)$ to the encoded phase values $\phi(x_m,y_m)$ and by multiplication of an encrypting amplitude value $a_c(x_m,y_m)$ with the encoded amplitude value $a(x_m,y_m)$,

Each mask resolution element (x_m,y_m) modulating the phase and the amplitude of electromagnetic radiation incident upon it with the complex value $a(x_m,y_m)a_c(x_m,y_m)e^{i\phi(xm,ym)+i\phi c(xm,ym)}$,

The system comprising

A source of electromagnetic radiation for emission of electromagnetic radiation for illumination of the mask,

A complex spatial electromagnetic radiation modulator that is positioned in the path of the electromagnetic radiation and comprising modulator resolution elements (x_d,y_d), each

modulator resolution element (x_d,y_d) modulating the phase and the amplitude of electromagnetic radiation incident upon it with a predetermined complex value $a_d(x_d,y_d)e^{i\phi d(xd,yd)}$, the decrypting phase value $\phi_d(x_d,y_d)$ and the decrypting amplitude value $a_d(x_d,y_d)$, respectively, of a modulator resolution element (x_d,y_d) being substantially equal to $-\phi_c(x_m,y_m)$ and $a_c^{-1}(x_m,y_m)$, respectively, of a corresponding mask resolution element (x_m,y_m), and

An imaging system for imaging the mask and the electromagnetic radiation modulator onto the image having the image intensity pattern $I(x',y')$.

29. A system according to claim 28, wherein the imaging system comprises a common path interferometer.

30. A system according to claim 28 or 29, wherein the imaging system comprises a phase contrast imaging system.

31. A system according to claim 29 or 30, further comprising

Means for Fourier or Fresnel transforming the electromagnetic radiation modulated by the mask and the complex spatial electromagnetic radiation modulator and being positioned on a propagation axis of the modulated radiation,

A spatial filter for filtering the Fourier or Fresnel transformed electromagnetic radiation by

In a region of spatial frequencies comprising DC in the Fourier or Fresnel plane,

Phase shifting with a predetermined phase shift value θ the modulated electromagnetic radiation in relation to the remaining part of the electromagnetic radiation, and

Multiplying the amplitude of the modulated electromagnetic radiation with a constant B, and

In a region of remaining spatial frequencies in the Fourier or Fresnel plane, multiplying the amplitude of the modulated electromagnetic radiation with a constant A,

Means for forming the intensity pattern by Fourier or Fresnel transforming, respectively, the phase shifted Fourier or Fresnel transformed modulated electromagnetic radiation, whereby each resolution element (x_m,y_m) of the mask is imaged on a corresponding resolution element (x',y') of the image,

The filtering parameters A, B, θ substantially fulfilling the equation

$$I(x',y') = A^2|a(x',y')e^{i\phi(x',y')} + \bar{\alpha}\,(BA^{-1}e^{i\theta}-1)|^2$$

For selected phase shift values θ, $\bar{\alpha}$ being the average of the complex phasors $a(x,y)e^{i\phi(x,y)}$.

32. A system according to claim 31, wherein the filtering parameters A and B substantially fulfil that A=1 and B=1, and for each (x,y) of the encoder: a(x,y)=1.

33. A system according to claim 32, wherein the phase shift value θ substantially fulfils the equation

$$|\bar{\alpha}| = \frac{1}{2|\sin\frac{\theta}{2}|}$$

34. A system according to claim 33, wherein the phase shift θ is substantially equal to π.

35. A system according to any of claims 30-33, further comprising

Means for moving the region of spatial frequencies comprising DC to a second part of the Fourier or Fresnel plane, and wherein

The spatial filter is adapted to phase shift the transformed modulated electromagnetic radiation at the second part of the Fourier or Fresnel plane by θ in relation to the remaining part of the electromagnetic radiation.

36. A system according to claim 35, wherein the means for moving the region of spatial frequencies comprising DC to a second part of the Fourier or Fresnel plane comprises an optical component, such as a grating, a prism, etc, with an appropriate carrier frequency.

37. A system according to any of claims 31-36, wherein the spatial filter comprises a spatial light modulator.

38. A system according to any of claims 31-37, wherein the spatial filter is adapted to perform the optical function of an output lens by appropriate encoding of the spatial filter.

39. A system according to any of claims 28-38, wherein the source of electromagnetic radiation is adapted to radiate electromagnetic radiation of different wavelengths corresponding to three different colours, such as red, green and blue, for generation of intensity patterns of arbitrary colours.

40. A system according to any of claims 31-39, further comprising a first and a second Fourier transforming lens, the mask being positioned in the front focal plane of the first lens, the spatial filter being positioned at the back focal plane of the first lens, and the second lens being positioned so that its front focal plane is positioned at the position of the back focal plane of the first lens.

41. A system according to any of claims 31-40, further comprising one Fourier transforming lens, the spatial filter being positioned at the back focal plane of the lens.

42. A system according to any of claims 31-41, further comprising one imaging lens, the spatial filter being positioned in the back focal plane of the lens.

43. A system according to any of claims 31-42, further comprising a polarising beam splitter and a quarter wave plate and/or a phase filter reflecting electromagnetic radiation incident upon it.

44. A system according to any of claims 31-43, wherein the spatial filter changes the phase of the radiation in the region of spatial frequencies comprising DC and leaves the phase of the remaining part of the radiation unchanged.

45. A system according to any of claims 31-43, wherein the spatial filter do not change the phase of the radiation in the region of spatial frequencies comprising DC and changes the phase of the remaining part of the radiation.

46. A system according to any of claims 31-43, wherein the spatial filter blocks the radiation at the region of spatial frequencies comprising DC and leaves the remaining part of the radiation unchanged.

47. A system according to any of claims 31-46, wherein the source of electromagnetic radiation is a Laser.

48. A system according to any of claims 28-47, wherein each of the encrypting phase values $\phi_c(x_m,y_m)$ is substantially equal to a value selected from a set consisting of two phase values.

49. A method according to claims 48, wherein each of the encrypting phase values $\phi_c(x_m,y_m)$ is substantially equal to a value selected from the set consisting of 0 and π.